Incident Response and SAP Systems

Juan Pablo Perez-Etchegoyen
jppereze@onapsis.com
@jp_pereze

Sergio Abraham
sabraham@onapsis.com
@serj_ab

Disclaimer

This presentation contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Onapsis Inc. Overview

Transforming how organizations protect the applications that manage their business-critical processes and information.

- **Founded:** 2009
- **Locations:** Buenos Aires, AR | Boston, MA | Berlin, DE | Lyon, FR
- **Technology**: Onapsis X1 (Auditor Solution)

  Onapsis Security Platform (Enterprise Solution)

  (PCT patent-pending)
- **Pricing:** Subscription-based (Enterprise, Audit On-Demand and MSP)
- **Research:** 130+ SAP security advisories and presentations published

Who are We?

- Juan Perez-Etchegoyen (JP) – CTO @ Onapsis
  - Background on Penetration Testing and vulnerabilities research
  - Reported vulnerabilities in different SAP and Oracle Products

- Sergio Abraham – SAP Security Specialist @ Onapsis
  - Reported vulnerabilities in different SAP Products
  - Worked on the support of HANA in Onapsis products

- Both Authors/Contributors on diverse posts and publications
- Speakers and Trainers at Information Security Conferences

Agenda

onapsis

- Incident Response
  - Concept
- First steps after any incident
  - Detection & Classification
  - Affected Assets
  - Legal actions
- Impact on SAP Systems
  - Prioritization
  - Affected information/processes
- Analysis phase
  - Logs, traces and tables
- Practical Scenario
- Conclusions

What should we expect out of this talk:

- Not a full/detailed Incident response procedure.
- Provides guidance and concepts around a complex topic (How to react and to proceed).
- Not a technical talk (do not expect any hardcore exploits)
- Not an hour talk.
- Open discussions by the end.
- Case study (not a real case) showing the analysis phase. Only relevant technical information is shown.

Incident Response | Concept

- Organizational approach to respond and manage the actions required to recover from an incident which is usually known as security breach or hack.
- Objectives:
  - Understand the root cause of the incident and the scope of the compromise
  - Limit damage (minimize impact)
    - Protect the company’s reputation
  - Recover (reducing time and costs)
    - keep processes running
  - Incorporate lessons learned (procedures/documentation)
    - Identify improvements to better protect the business processes

First Steps | Detection

- ❑ *What happened?*
  - *Analysis of the symptom/s*
    - *“There are users created in production that we don’t know where they came from”*
    - *“An email with confidential HR information is being distributed to employees”*
    - *“Disclosure of our long-term marketing strategy, which should be confidential”*
- ❑ *What’s the severity of the incident?*
  - *Dimension of the impact*
    - *There are SAP_ALL users in production, they can do whatever they want!*
    - *Legal consequences and regulations might apply.*
    - *The company’s image can be affected.*

Incident Response | Classification

- ❑ Availability -> Sabotage
  - SAP System/service is ***down and/or inoperable***
    - *“ERP System is down”*
    - *“Customer service interface is not working”*
- ❑ Confidentiality -> Espionage
  - SAP System information was ***leaked***
    - *“Employees salary is being spread through emails”*
    - *“Social Security Numbers and Bank accounts have been published on the Internet”*
- ❑ Integrity -> Fraud
  - SAP System information was ***altered***
    - *“Employees are not receiving their salary, bank accounts… changed?”*
    - *“Balances are suspiciously inconsistent”*

First Steps | Affected Assets

- ❑ Assets can be represented in several ways:
  - A piece of information
  - A physical server
  - An SAP System
  - A database
  - One instance of an SAP System

- ❑ Affected Assets…
  - ❑… should be chosen based on the symptoms
  - ❑ … will define the **scope** of an Incident Response Project

First Steps | Legal actions

- ❑ **Do we intend to prosecute? It is a one chance decision.**

Not To Prosecute	To Prosecute
Simpler processes/investigations	Formal Investigation
Money: Less expensive	Money: Expensive
Time: Less expensive	Time: Expensive

- ❑ **Chain Of Custody** :
  - It includes security response teams, 3rd party specialists, law enforcement, white rooms, and so on.
  - Implementing Chain of Custody in SAP environments is a **real challenge**. It requires states preservation, assets isolation, etc.
  - Evidence must be admissible in court: reliable, usable, authenticated and integral
  - In the end the person who is going to decide whether a piece of evidence is admissible for the court are the lawyers/prosecutors/judges.

Impact on SAP Systems | Prioritize

- ❑ Are all SAP Systems equally important?

- ❑Huge amount of data -> Need of prioritization

- ❑ Start by the most critical assets.
  - Most critical business processes
  - Daily transactions systems + Sensitive Data (ERP, HR)
  - Key technical and security systems (SolMan, GRC)
  - Highly interfaced systems (BW, PI)

- ❑ Focus on Productive environments (but do not exclude the rest of the landscape, DEV/QA could be important too)

Impact on SAP Systems | Impact

- Having identified the affected assets and prioritized the SAP Systems: **Which information is at risk?**

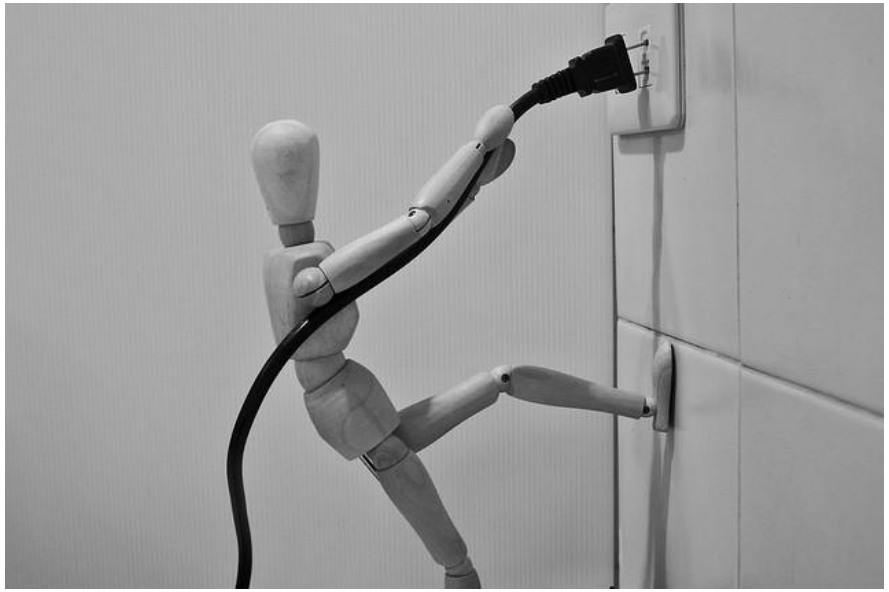
- Sensitive information in SAP Systems:
  - Social Security Number
  - Salary
  - Credit Cards
  - Health Insurance
  - Product Formulas
  - Bank accounts
  - Intellectual Property
  - Customer/Supplier data

- Data must have been previously classified in order to measure the risk exposure.
- What is the impact of disclosure or losing this information?
- How do we react to these threats?

Analysis phase

- Forensics theory:

Incident -> Keep the last state -> Take images



In order to keep the last state we actually need to **UNPLUG** the host

In SAP, this is not a good idea!

Analysis phase (contd)

Mechanism	Location
Security Audit Log	/usr/sap/**<SID>/<INSTANCE>**/log/audit_**date**
Developer traces	Directory: /usr/sap/**<SID>/<INSTANCE>**/work/dev_*
System Log	/usr/sap/**<SID>/<INSTANCE>**/log/SLOG**<SYSNR>**
System Trace	/usr/sap/**<SID>/<INSTANCE>**/log/TRACE
Gateway Log	/usr/sap/**<SID>/<INSTANCE>**/work/<file_name> **<file_name>** is defined by key **LOGFILE**
Web Dispatcher Log	Specified by parameter **icm/HTTP/logging_XX**
WD Security Log	/usr/sap/**<SID>/<INSTANCE>**/work/dev_icm_sec
Table Change Logging	Table DBTABLOG
User & Auth.	Tables USH02, USH04, USH10, USH12…
ABAP Change Doc.	Tables CDHDR, CDPOS

Case Study

Salaries has been distributed among employees

Case Study: Salaries were published

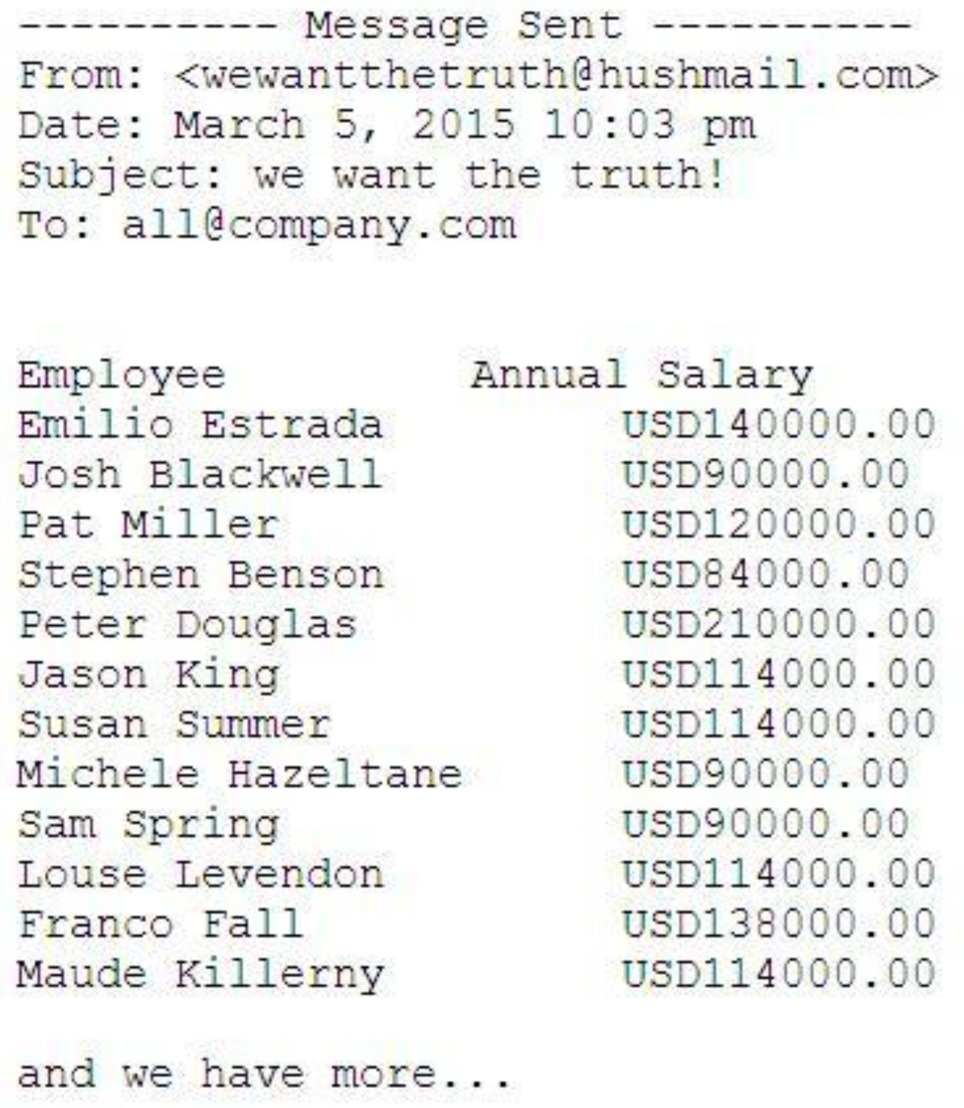
- ❑ This information has been distributed in an e-mail among all employees

High confidential information has been leaked!

Symptom

It will get some people very angry.

In fact, it will totally affect the work environment!



---------- Message Sent ----------
From: <wewantthetruth@hushmail.com>
Date: March 5, 2015 10:03 pm
Subject: we want the truth!
To: all@company.com

Employee	Annual Salary
Emilio Estrada	USD140000.00
Josh Blackwell	USD90000.00
Pat Miller	USD120000.00
Stephen Benson	USD84000.00
Peter Douglas	USD210000.00
Jason King	USD114000.00
Susan Summer	USD114000.00
Michele Hazeltane	USD90000.00
Sam Spring	USD90000.00
Louse Levendon	USD114000.00
Franco Fall	USD138000.00
Maude Killerny	USD114000.00

and we have more...

Case Study: Salaries were published

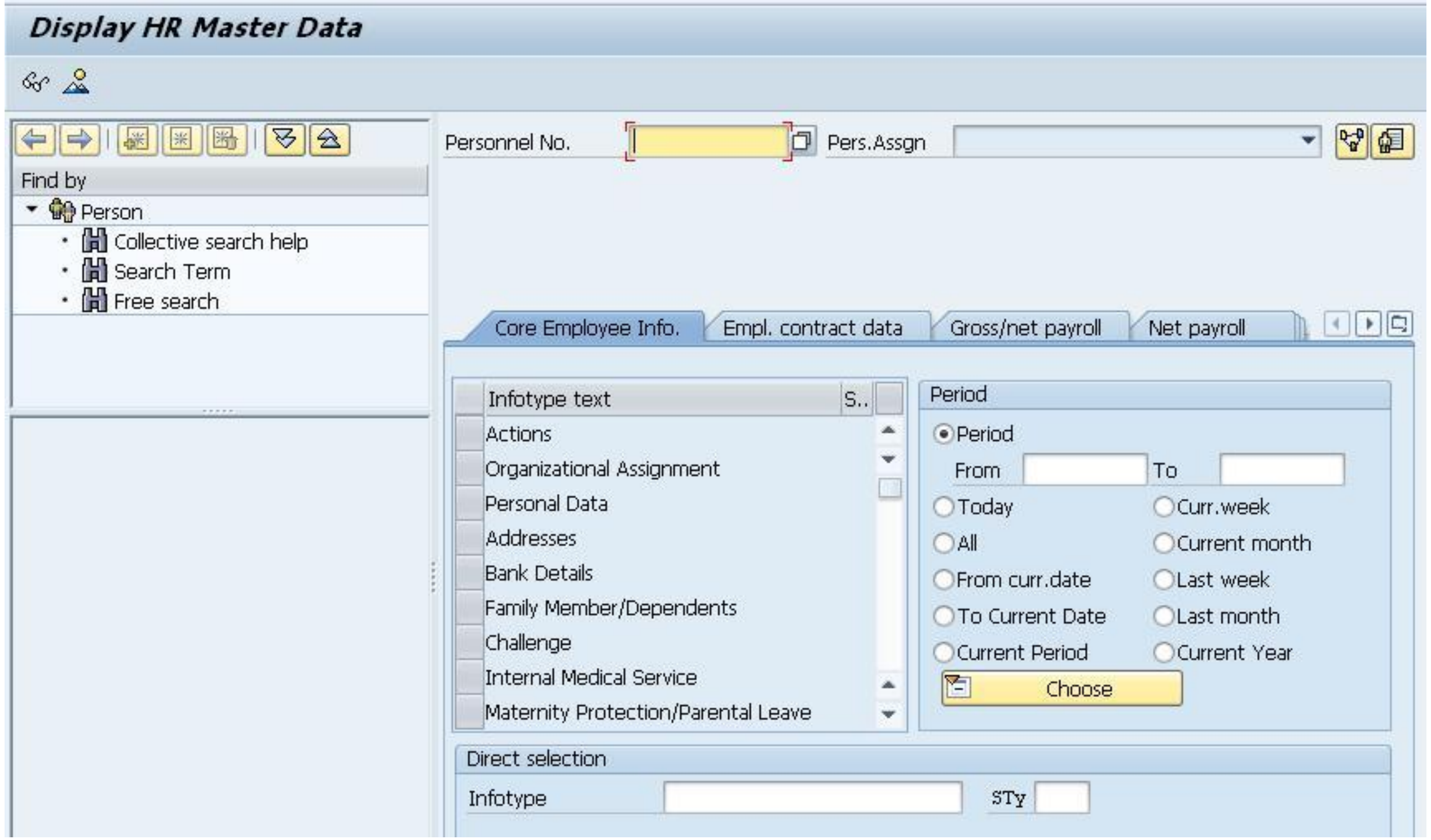
- ❑ **This information is on the SAP HR system. As a first approach, that should be the source we will look at (e.g.: HR1 was compromised).**
- ❑ **Other systems interfacing with HR1 should also be analyzed …ERP? BW? GRC?**

- ❑ **Two big tasks:**
  - ▪ Go to the root of the issue: Was HR1 compromised? How? By whom? Is there evidence of a backdoor?
  - ▪ Analyze the potential extent of the compromise (other systems).

Case Study: Salaries were published

- **HR1:** Salaries information is located in table PA0008, and can be also commonly accessed using transaction PA20 or report RPLEHSU0.
- Summary: We have three starting points.
  - Transaction PA20
  - Table PA0008
  - Report RPLEHSU0

Check accesses to these objects and trace back their execution.



Display HR Master Data

Personnel No. | Pers.Assgn

Find by
- Person
  - Collective search help
  - Search Term
  - Free search

Core Employee Info. | Empl. contract data | Gross/net payroll | Net payroll

Infotype text	S..
Actions	
Organizational Assignment	
Personal Data	
Addresses	
Bank Details	
Family Member/Dependents	
Challenge	
Internal Medical Service	
Maternity Protection/Parental Leave	

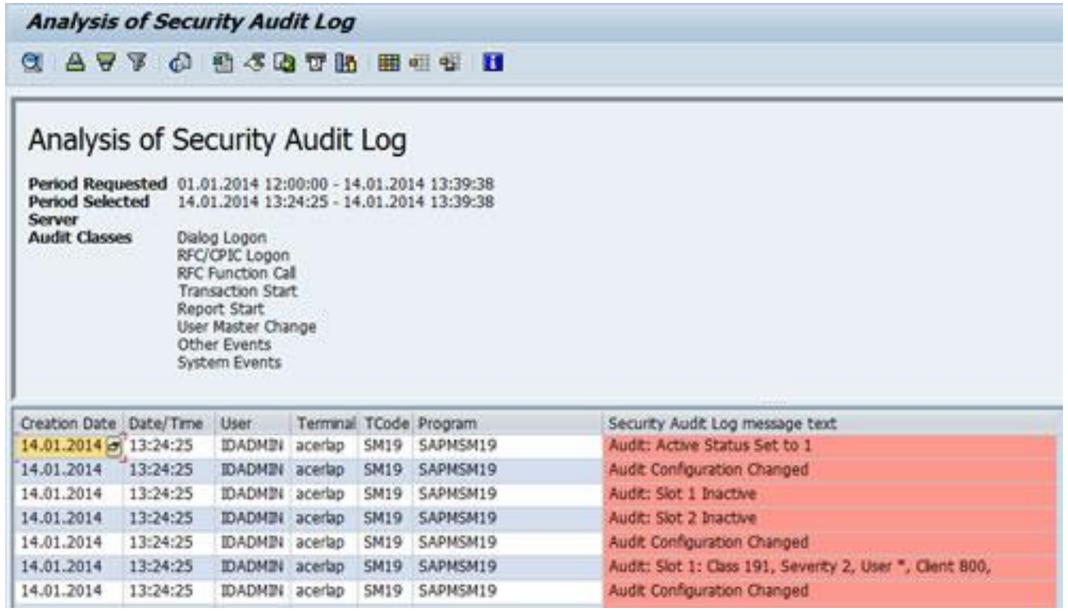
Period
- ● Period
- From | To
- ○ Today ○ Curr.week
- ○ All ○ Current month
- ○ From curr.date ○ Last week
- ○ To Current Date ○ Last month
- ○ Current Period ○ Current Year
- Choose

Direct selection
Infotype | STy

Case Study: Salaries were published

- ❑ Check the version of HR1 SAP System (different SAP Versions have different audit and trace features)
- ❑ List all the available sources of information which can be useful to find the execution of transaction or reports and the reading of tables.
    - Security Audit Log
    - STAD

These are not the only sources available.

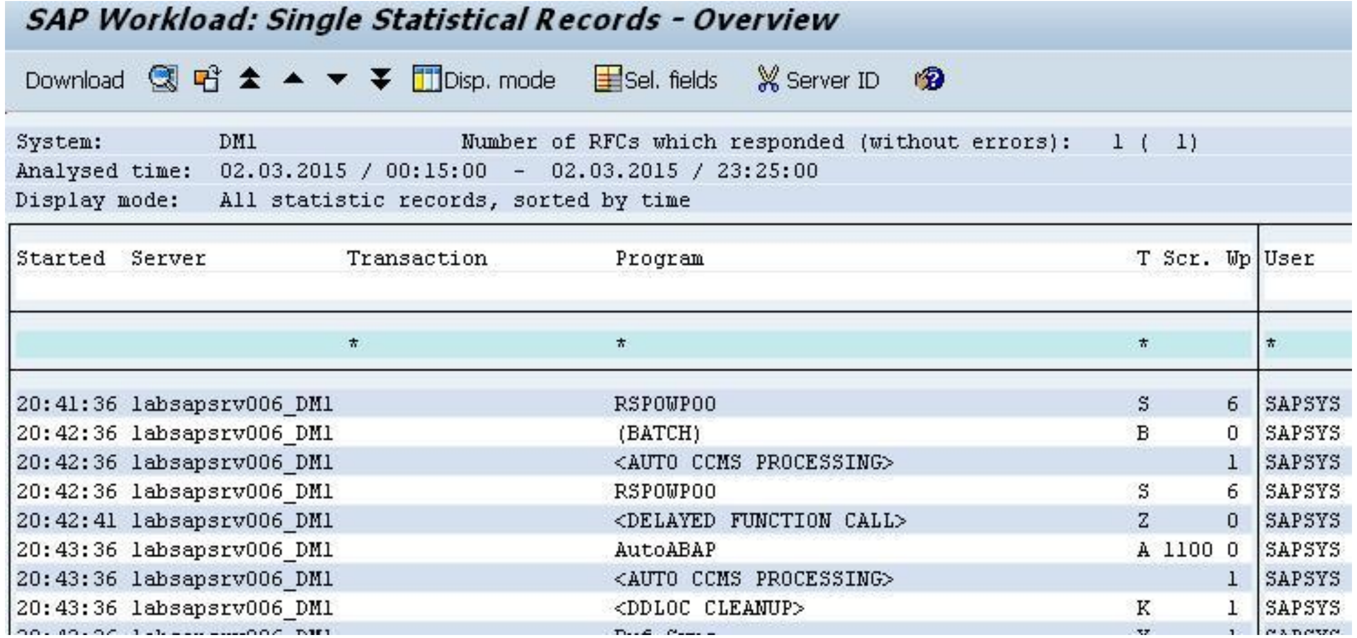


Analysis of Security Audit Log

Analysis of Security Audit Log

Period Requested	01.01.2014 12:00:00 - 14.01.2014 13:39:38
Period Selected	14.01.2014 13:24:25 - 14.01.2014 13:39:38
Server	
Audit Classes	Dialog Logon RFC/CPIC Logon RFC Function Call Transaction Start Report Start User Master Change Other Events System Events

Creation Date	Date/Time	User	Terminal	TCode	Program	Security Audit Log message text
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit: Active Status Set to 1
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit Configuration Changed
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit: Slot 1 Inactive
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit: Slot 2 Inactive
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit Configuration Changed
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit: Slot 1: Class 191, Severity 2, User *, Client 800,
14.01.2014	13:24:25	IDADMIN	acerlap	SM19	SAPMSM19	Audit Configuration Changed

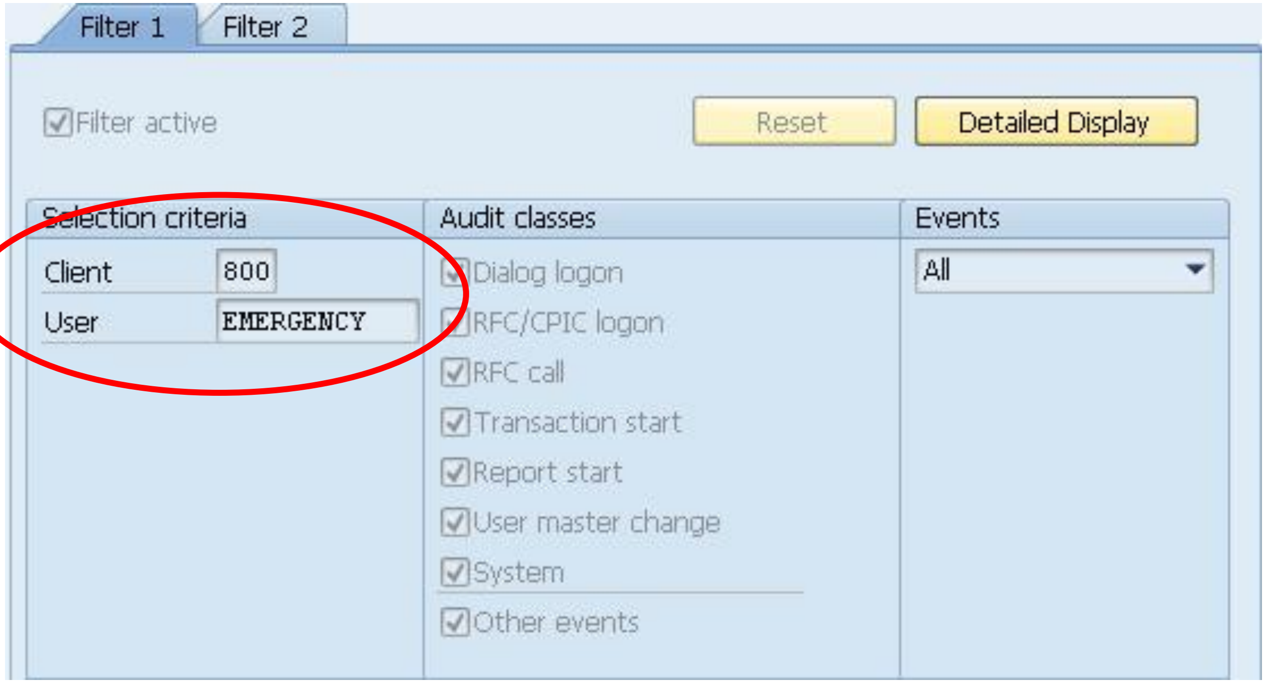


SAP Workload: Single Statistical Records - Overview

```
System:          DM1              Number of RFCs which responded (without errors):   1 (  1)
Analysed time:   02.03.2015 / 00:15:00  -  02.03.2015 / 23:25:00
Display mode:    All statistic records, sorted by time

Started  Server             Transaction          Program                                  T Scr. Wp User

                                   *                    *                                   *        *

20:41:36 labsapsrv006_DM1                        RSPOWP00                                 S      6 SAPSYS
20:42:36 labsapsrv006_DM1                        (BATCH)                                  B      0 SAPSYS
20:42:36 labsapsrv006_DM1                        <AUTO CCMS PROCESSING>                          1 SAPSYS
20:42:36 labsapsrv006_DM1                        RSPOWP00                                 S      6 SAPSYS
20:42:41 labsapsrv006_DM1                        <DELAYED FUNCTION CALL>                  Z      0 SAPSYS
20:43:36 labsapsrv006_DM1                        AutoABAP                                 A 1100 0 SAPSYS
20:43:36 labsapsrv006_DM1                        <AUTO CCMS PROCESSING>                          1 SAPSYS
20:43:36 labsapsrv006_DM1                        <DDLOC CLEANUP>                          K      1 SAPSYS
```

Case Study: Salaries were published

- Security Audit Log
  - Check SM19 for Security Audit Log Events configuration



☑ Filter active

Selection criteria

Client 800

User EMERGENCY

Audit classes

☑ Dialog logon

☑ RFC/CPIC logon

☑ RFC call

☑ Transaction start

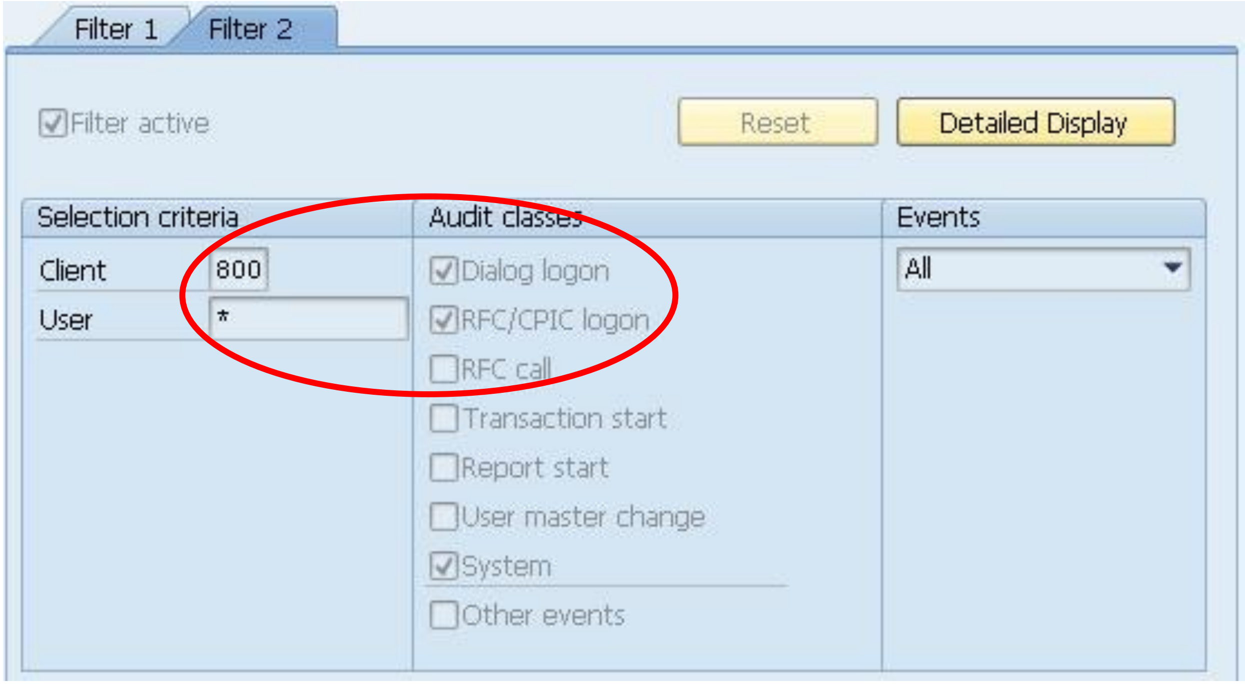
☑ Report start

☑ User master change

☑ System

☑ Other events

Events: All



☑ Filter active

Selection criteria

Client 800

User *

Audit classes

☑ Dialog logon

☑ RFC/CPIC logon

□ RFC call

□ Transaction start

□ Report start

□ User master change

☑ System

□ Other events

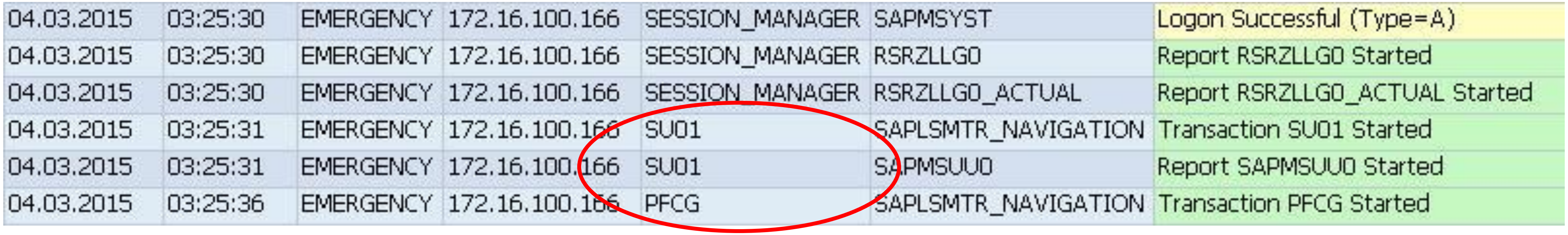
Events: All

We will have ALL events only for EMERGENCY user and

for the rest of the users only Logon events.

Case Study: Salaries were published

- Security Audit Log
  - Check SM20.
  - We can only see if EMERGENCY user executed PA20, RPLEHSU0 or read PA0008



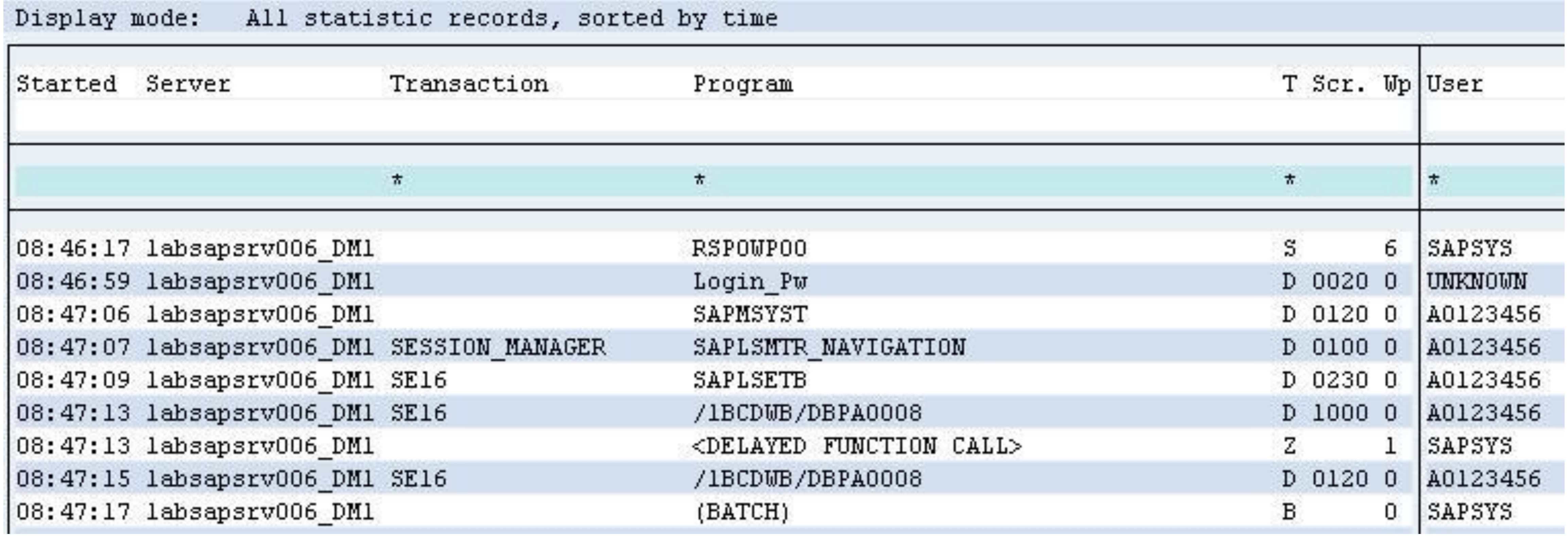
04.03.2015	03:25:30	EMERGENCY	172.16.100.166	SESSION_MANAGER	SAPMSYST	Logon Successful (Type=A)
04.03.2015	03:25:30	EMERGENCY	172.16.100.166	SESSION_MANAGER	RSRZLLG0	Report RSRZLLG0 Started
04.03.2015	03:25:30	EMERGENCY	172.16.100.166	SESSION_MANAGER	RSRZLLG0_ACTUAL	Report RSRZLLG0_ACTUAL Started
04.03.2015	03:25:31	EMERGENCY	172.16.100.166	SU01	SAPLSMTR_NAVIGATION	Transaction SU01 Started
04.03.2015	03:25:31	EMERGENCY	172.16.100.166	SU01	SAPMSUU0	Report SAPMSUU0 Started
04.03.2015	03:25:36	EMERGENCY	172.16.100.166	PFCG	SAPLSMTR_NAVIGATION	Transaction PFCG Started

We have the clue that EMERGENCY user accessed to user management transactions, but didn’t use any of the objects we are looking for.

- **First user to take into account: EMERGENCY in client 800 and an IP address**
- **First actions:**
  - **Check if that IP is from a valid user.**
  - **Check the policy of EMERGENCY user access**

Case Study: Salaries were published

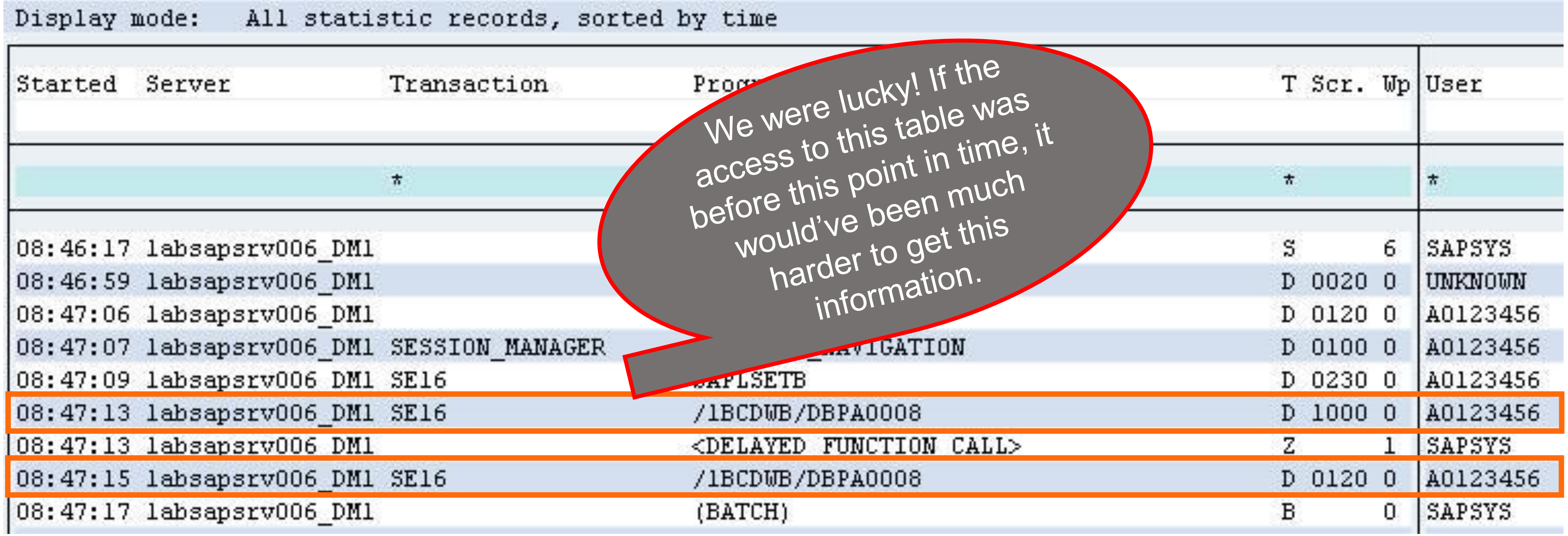
- STAD
  - It only “adds” information. If the information is retrieved quickly (48 hours by default) after the incident, then it can be useful to trace back activities on the system.



```
Display mode:   All statistic records, sorted by time

Started  Server           Transaction      Program                     T Scr. Wp User

                          *                *                           *         *

08:46:17 labsapsrv006_DM1                 RSPOWP00                    S       6 SAPSYS
08:46:59 labsapsrv006_DM1                 Login_Pw                    D 0020 0 UNKNOWN
08:47:06 labsapsrv006_DM1                 SAPMSYST                    D 0120 0 A0123456
08:47:07 labsapsrv006_DM1 SESSION_MANAGER SAPLSMTR_NAVIGATION         D 0100 0 A0123456
08:47:09 labsapsrv006_DM1 SE16            SAPLSETB                    D 0230 0 A0123456
08:47:13 labsapsrv006_DM1 SE16            /1BCDWB/DBPA0008            D 1000 0 A0123456
08:47:13 labsapsrv006_DM1                 <DELAYED FUNCTION CALL>     Z       1 SAPSYS
08:47:15 labsapsrv006_DM1 SE16            /1BCDWB/DBPA0008            D 0120 0 A0123456
08:47:17 labsapsrv006_DM1                 (BATCH)                     B       0 SAPSYS
```

Case Study: Salaries were published

- STAD
  - It also allows to get more in-depth information that could be very useful!



```
Display mode:   All statistic records, sorted by time

Started  Server            Transaction       Prog                                T Scr.  Wp  User

                                 *                                               *           *

08:46:17 labsapsrv006_DM1                                                        S       6   SAPSYS
08:46:59 labsapsrv006_DM1                                                        D 0020  0   UNKNOWN
08:47:06 labsapsrv006_DM1                                                        D 0120  0   A0123456
08:47:07 labsapsrv006_DM1 SESSION_MANAGER                      _NAVIGATION        D 0100  0   A0123456
08:47:09 labsapsrv006_DM1 SE16              SAPLSETB                             D 0230  0   A0123456
08:47:13 labsapsrv006_DM1 SE16              /1BCDWB/DBPA0008                     D 1000  0   A0123456
08:47:13 labsapsrv006_DM1                   <DELAYED FUNCTION CALL>              Z       1   SAPSYS
08:47:15 labsapsrv006_DM1 SE16              /1BCDWB/DBPA0008                     D 0120  0   A0123456
08:47:17 labsapsrv006_DM1                   (BATCH)                              B       0   SAPSYS
```

We were lucky! If the access to this table was before this point in time, it would've been much harder to get this information.

- It seems user **A0123456** used **SE16** to read table **PA0008**. Just double-click on the row.

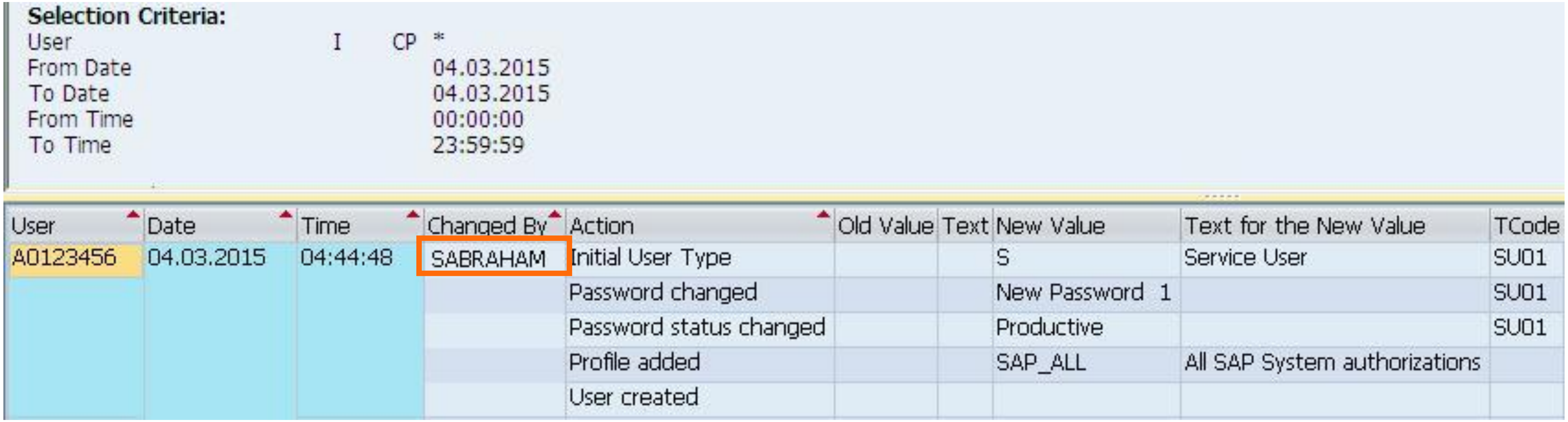
Case Study: Salaries were published

- Summary
  - **EMERGENCY** user was used without requesting it, but at the naked eye, didn't do much.
  - An IP Address from where the EMERGENCY user was connected **172.16.100.166**.
  - There is an unknown user called **A0123456** which actually accessed to table **PA0008** from SE16 transaction.

- Next steps:
  - Trace back the creation of user A0123456.
  - Was the system compromised? How?
  - Is there evidence of a backdoor?

Case Study: Salaries were published

- SUIM Change Documents
  - This report will show exactly who created the user **A0123456**.



Selection Criteria:

User	I	CP	*
From Date			04.03.2015
To Date			04.03.2015
From Time			00:00:00
To Time			23:59:59

User	Date	Time	Changed By	Action	Old Value	Text	New Value	Text for the New Value	TCode
A0123456	04.03.2015	04:44:48	SABRAHAM	Initial User Type			S	Service User	SU01
				Password changed			New Password 1		SU01
				Password status changed			Productive		SU01
				Profile added			SAP_ALL	All SAP System authorizations	
				User created					

Due to the lack of Security Audit Log events, this is the only information available.

Table USR02 will show also who created it, but this report collects more information.

Case Study: Salaries were published

❑ The user belongs to an employee on vacations. He couldn’t do it.

❑ Hypothesis: Could someone have used the account instead?

❑ His office remained closed with a key. It seems that nobody should have been able to get to his office and use his computer.

❑ It could have been done from another host, potentially: **172.16.100.166**.

❑ EMERGENCY user connected without being authorized

❑ **Would have somebody obtained both credentials?**

❑ Next task:

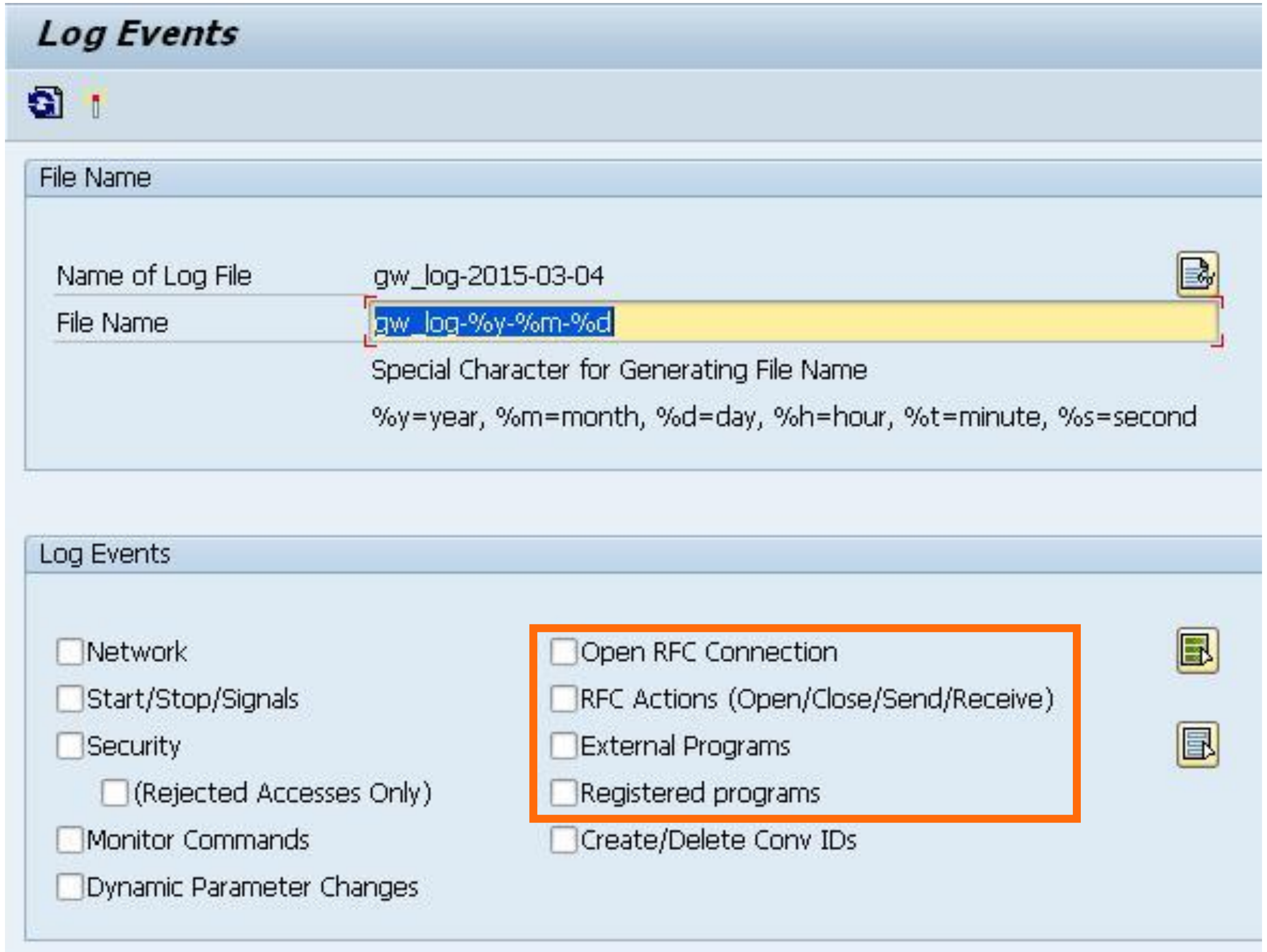
- Check low hanging fruit issues that could provide access to the SAP System
  - SAPXPG remote command execution?
  - Oracle External Authentication?
  - Any other unauthorized accesses to operating system level or database level?

Case Study: Salaries were published

- SAPXPG Remote Command Execution
  - Gateway Logging: Transaction SMGW -> Goto -> Expert Functions -> Logging

Gateway Logging would show valuable information related to external servers, and remote connections.

Sadly, these events are not enabled



Log Events

File Name

Name of Log File gw_log-2015-03-04

File Name gw_log-%y-%m-%d

Special Character for Generating File Name

%y=year, %m=month, %d=day, %h=hour, %t=minute, %s=second

Log Events

□ Network
□ Start/Stop/Signals
□ Security
□ (Rejected Accesses Only)
□ Monitor Commands
□ Dynamic Parameter Changes

□ Open RFC Connection
□ RFC Actions (Open/Close/Send/Receive)
□ External Programs
□ Registered programs
□ Create/Delete Conv IDs

Case Study: Salaries were published

- Oracle External Authentication
  - Check Listener.log
  - /oracle/<SID>/saptrace/diag/tnslsnr/<server_name>/listener/ (Oracle 11g)

```
03-MAR-2015 09:36:34 *
(CONNECT_DATA=(SERVICE_NAME=DM1)(CID=(PROGRAM=C:\instantclient_11_2\sqlplus.exe)
(HOST=1C943B28)(USER=dm1adm))) *
(ADDRESS=(PROTOCOL=tcp)(HOST=172.16.100.166)(PORT=1299)) * establish * DM1 * 0
```

An unauthorized user connected using the external authentication and <SID>adm user

It means that most likely the attacker had full access to the database. He could have left backdoors behind.

Case Study: Salaries were published

- Summary
  - After tracking down 172.16.100.166 IP address, IT team identified it and it belongs to a shared computer used for diverse purposes.
  - The attacker gained full access to the database: he/she may have had access to the USR02 table, potentially cracking user passwords (i.e. SABRAHAM and EMERGENCY). The extent of the compromise could have gone beyond these users, getting more sensitive information.
  - The attacker has knowledge of SAP Attacks, SAP Transactions and tables.
  - In fact, if the attacker got access to the database, why creating a user in SAP and used SE16 to read PA0008? Other possible actions performed by the attacker should also be analyzed.

- Next Steps
  - Delete user A0123456. Check validity of ALL users and change ALL passwords.
  - Check user activity on other systems (usually shared passwords may appear)
  - RFC Destinations to other systems. Check for incoming calls from HR1 in adjacent Systems.
  - Check Business and Technical data integrity.

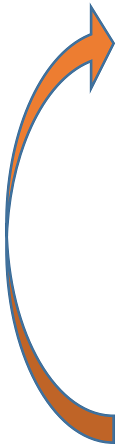
Case Study: Salaries were published

- Check integrity (perform integrity hash comparisons)
  - Check procedures code
  - Check triggers code
  - Check functions code
  - Check security-related parameters in database and SAP
  - Check REPOSRC table (ABAP Code) → REPOLOAD table can be refreshed after a system restart
  - Check the integrity of your business data

Go alive again!

Wrapping up

- Incident Response is all about the **process, where every step must be documented**:
  - Detection of the incident
  - Classification of the incident
  - Decision on legal actions
  - Hypothesis of affected Assets
  - Hypothesis of affected information (risk exposure)
  - Assets Prioritization
  - Information extraction phase → (live forensics)
  - Analysis phase
  - Lessons learned



Conclusions

- An Incident Response Process is **key** in corporate environments.
- SAP Systems hold the **most valuable information** in the company, therefore they **must be** part of our company Incident Response Process.
- If an incident is detected, the **whole landscape** could be the scope of the analysis, not just Productive environments.
- There is no much experience and documentation around Incident Response on SAP systems. It requires very specific skills and knowledge of **SAP logging features and limitations**.
- Though there are only a few Incidents related to SAP systems hitting the news, **they exist because of the criticality of its information**. Confidentiality is a key requirement of these projects.

Open questions…

- As in this example, finding the root cause and/or the origin is not always possible.
- There are some challenges regarding accessibility to the information.
    - Are the systems patched, so we can rely on the logging mechanisms?
    - Are the logs always there?
    - Do the stored logs have a validity period?
    - Are the logs deleted after a certain period of time?
    - Are the logs sent to a centralized location?
    - How much time after the incident, the incident response was triggered?
- Is an interdisciplinary team required? Should SAP and non-SAP teams work together?
- **Experience around SAP Incident Response in the audience?**
    - Happened to your company (hopefully not)
    - Helping an SAP customer to identify the root cause

References

- Previous Troopers conferences:
  - SAP Forensics (2013)
  - SAP Anti-Forensics (2014)
  - BIZEC Workshop (2015)
- Security Audit Log: https://help.sap.com/saphelp_nw74/helpdata/en/4D/41BEC4AA601C86E10000000A42189B/frameset.htm
- STAD: http://help.sap.com/saphelp_nw70/helpdata/en/c1/0dbf62e04311d286d6006008b32e84/content.htm
- SUIM Change Documents: http://help.sap.com/saphelp_nw70ehp2/helpdata/en/90/c3e45b841f214ca32fcc17f7eb059e/content.htm
- Gateway Logging: http://help.sap.com/saphelp_nw73ehp1/helpdata/en/48/b2a710ca1c3079e10000000a42189b/content.htm
- Listener.log (Oracle): http://docs.oracle.com/cd/B10501_01/network.920/a96580/troubles.htm#444555
- **Special thanks to Nahuel Sanchez and the Onapsis Research Labs!**

Questions?

Juan Pablo Perez-Etchegoyen
jppereze@onapsis.com
@jp_pereze

Sergio Abraham
sabraham@onapsis.com
@serj_ab