ONAPSIS

TROOPERS

SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

28-29 June 2023 | Yvan Genuer

Disclaimer

- This presentation contains references to the products of SAP SE. 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 SE 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.

Yvan Genuer

Security Researcher

ONAPSIS

Yvan Genuer

Security Researcher

ONAPSIS

20 years XP on SAP

10 years only SAP Security

100+ vulnerabilities reported

0 defensive talk

Yvan Genuer

Security Researcher

ONAPSIS

20 years XP on SAP

10 years only SAP Security

100+ vulnerabilities reported

~~0~~ 1 defensive talk

AGENDA

0x01 Why SAP Forensic ?

0x02 The White Paper

0x03 SAP Data Sources

0x04 Good to know…

0x05 Closing part

AGENDA

0x01	**Why SAP Forensic ?**
0x02	The White Paper
0x03	SAP Data Sources
0x04	Good to know…
0x05	Closing part

Why SAP Forensic ?

87%

of the Global 2000 use SAP

77%

of the world’s transaction revenue

100%

of F500 Oil & Gas

Why SAP Forensic ?

Espionage

Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.

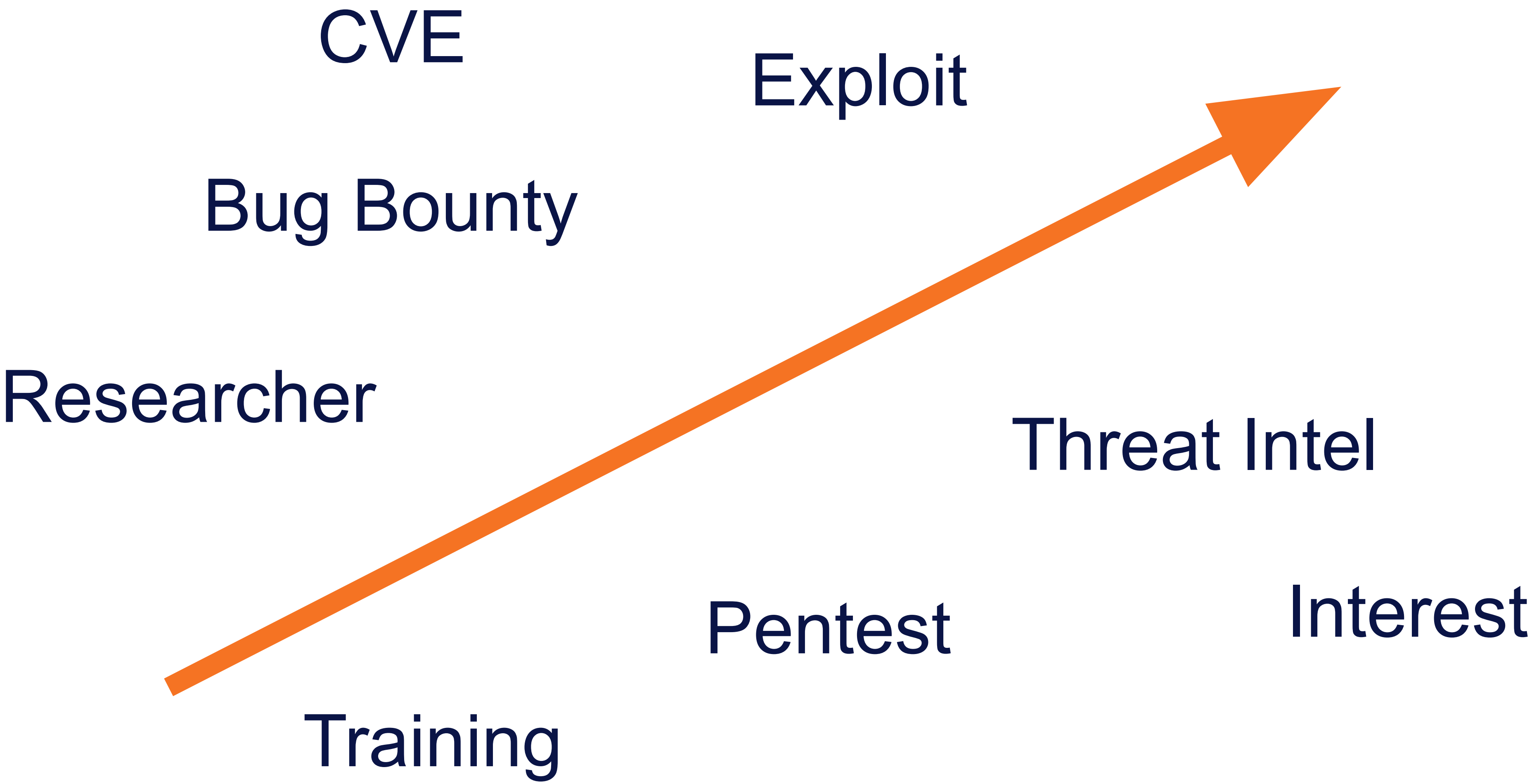
Sabotage

Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.

Fraud

Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

Why SAP Forensic ?



CVE

Exploit

Bug Bounty

Researcher

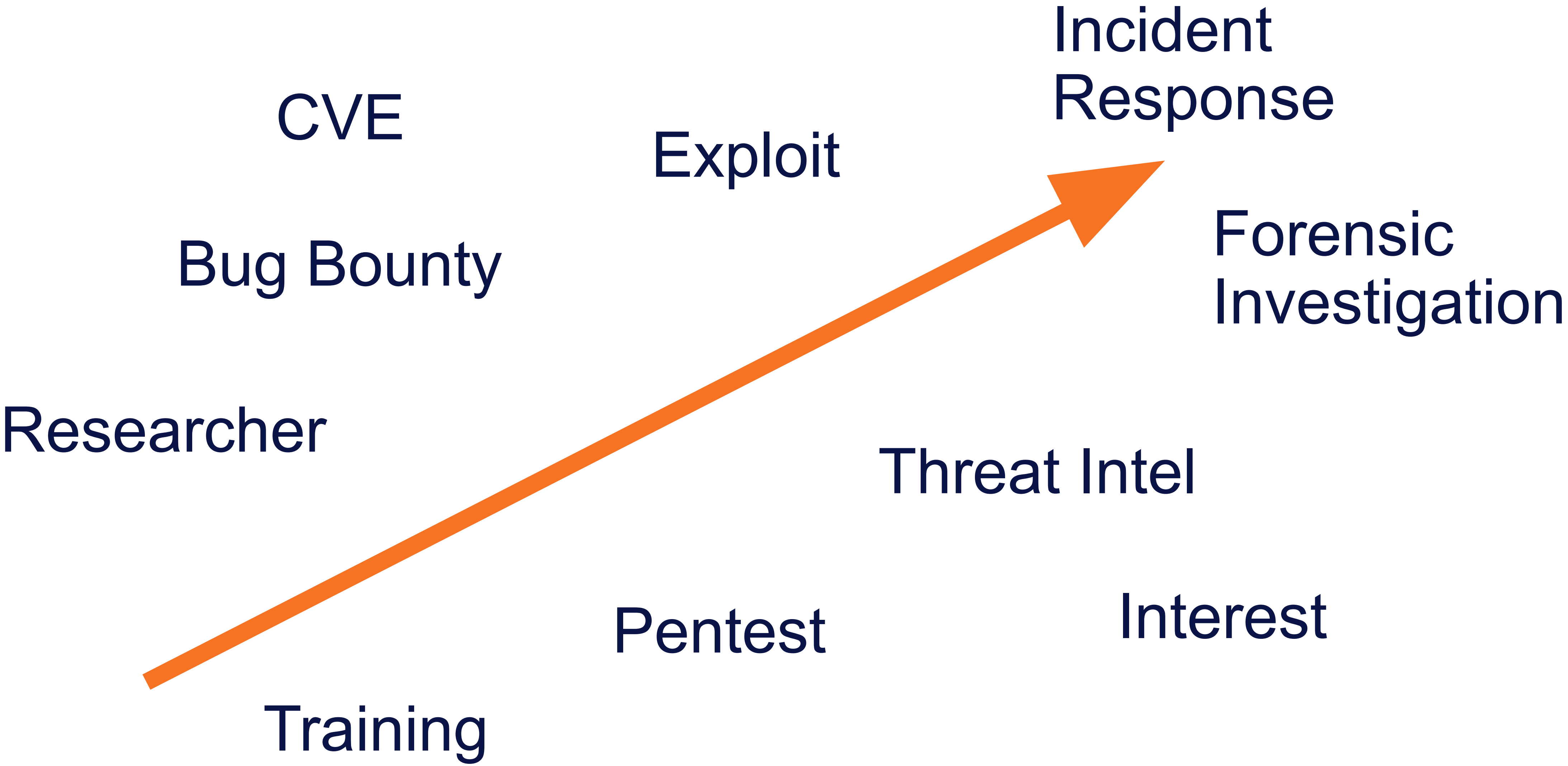
Threat Intel

Pentest

Interest

Training

Why SAP Forensic ?



Incident Response

CVE

Exploit

Forensic Investigation

Bug Bounty

Researcher

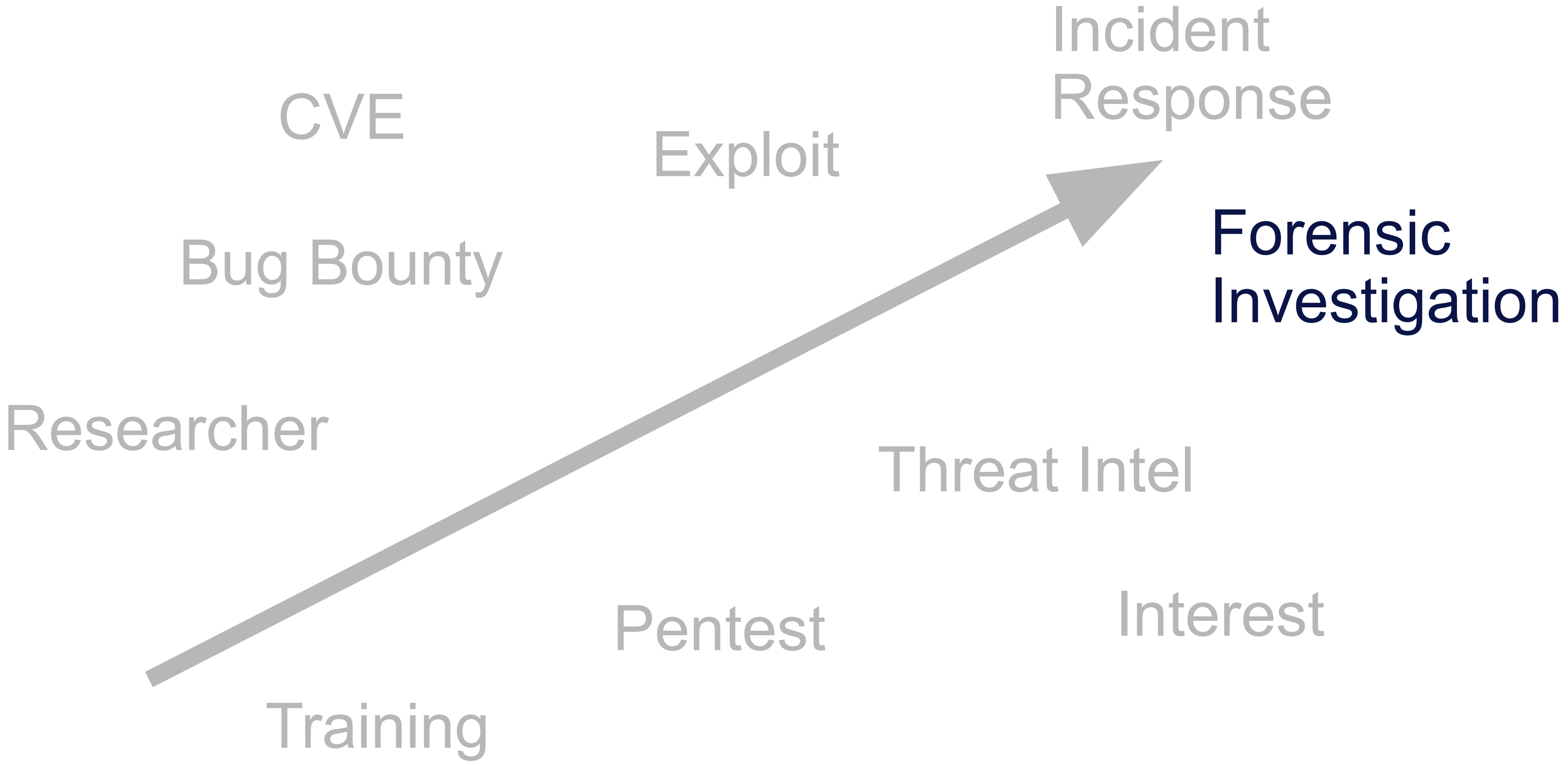
Threat Intel

Interest

Pentest

Training

Why SAP Forensic ?



Incident Response

CVE

Exploit

Forensic Investigation

Bug Bounty

Researcher

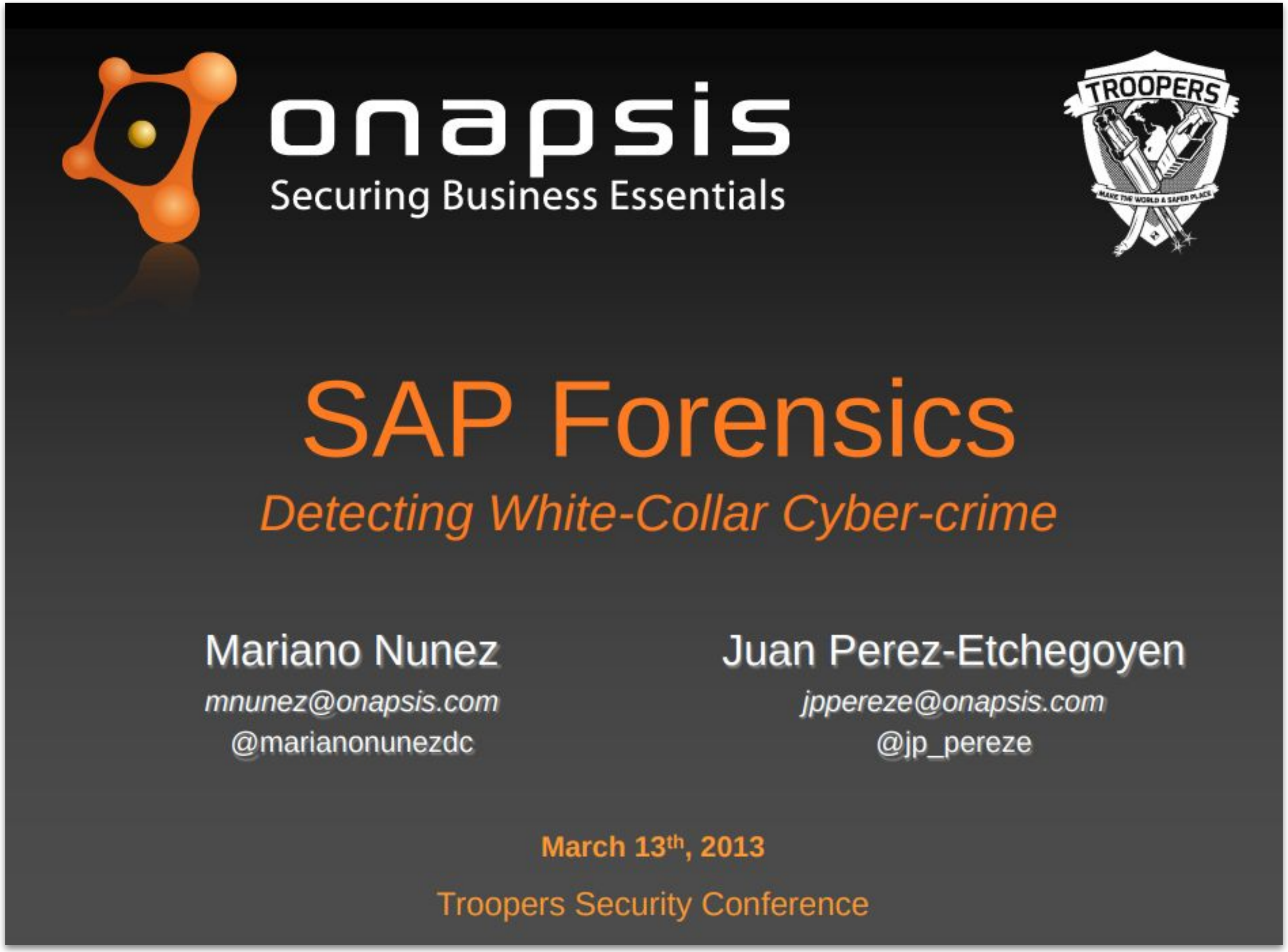
Threat Intel

Interest

Pentest

Training

Why SAP Forensic ?



onapsis
Securing Business Essentials

SAP Forensics

Detecting White-Collar Cyber-crime

Mariano Nunez
mnunez@onapsis.com
@marianonunezdc

Juan Perez-Etchegoyen
jppereze@onapsis.com
@jp_pereze

March 13th, 2013

Troopers Security Conference

2013

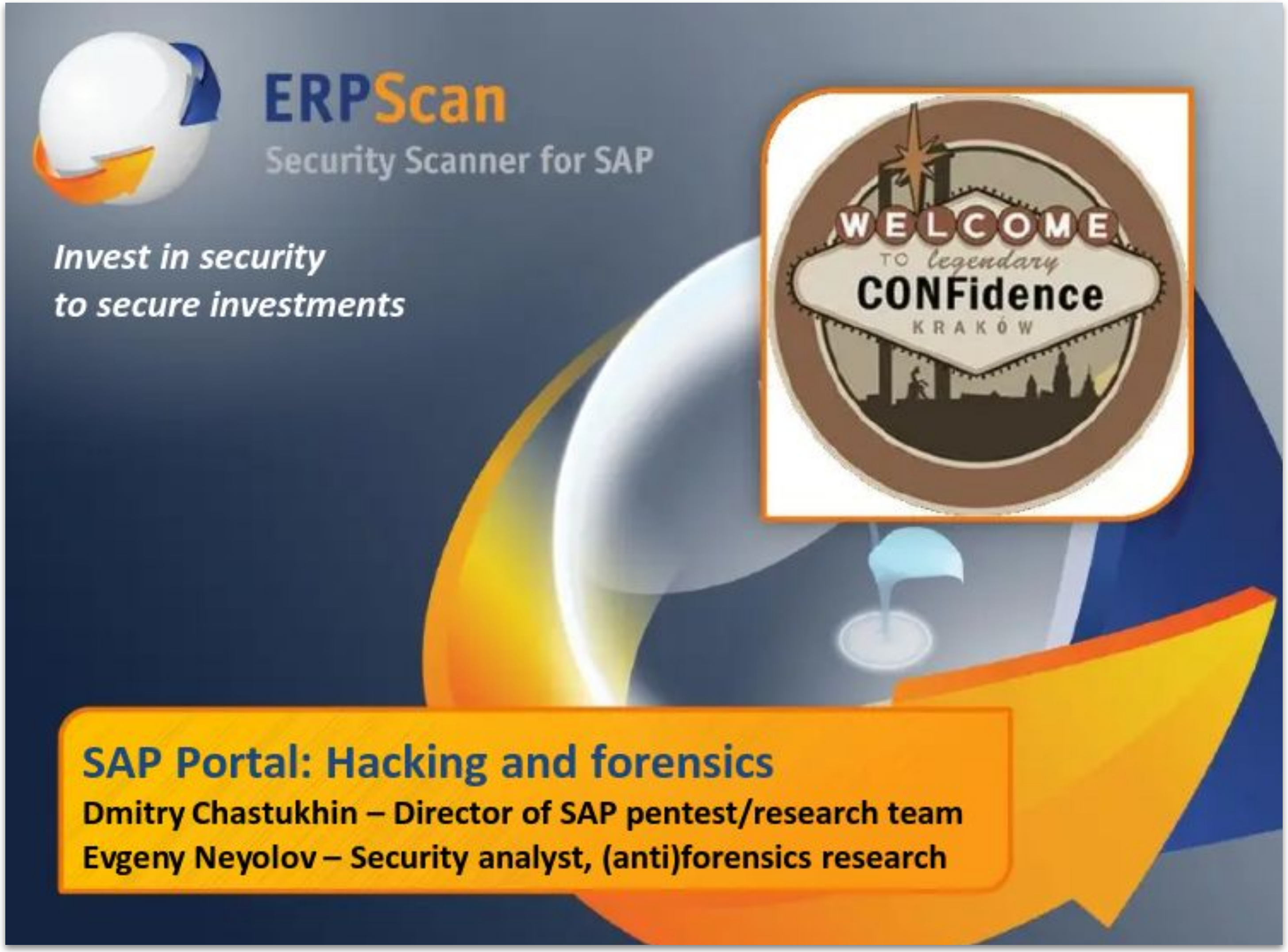
Onapsis

Mariano Nunez
Juan Perez-Etchegoyen

Highlight few important point already

https://troopers.de/media/filer_public/45/27/4527f0d5-d4ca-40c1-83c6-f0b81bb82518/troopers13-detecting_white-collar_cybercrime_sap_forensics-juan_perez-etchegoyenmariano_nunez.pdf

Why SAP Forensic ?



ERPScan

Security Scanner for SAP

Invest in security
to secure investments

WELCOME
TO legendary
CONFidence
KRAKÓW

SAP Portal: Hacking and forensics

Dmitry Chastukhin – Director of SAP pentest/research team

Evgeny Neyolov – Security analyst, (anti)forensics research

2013

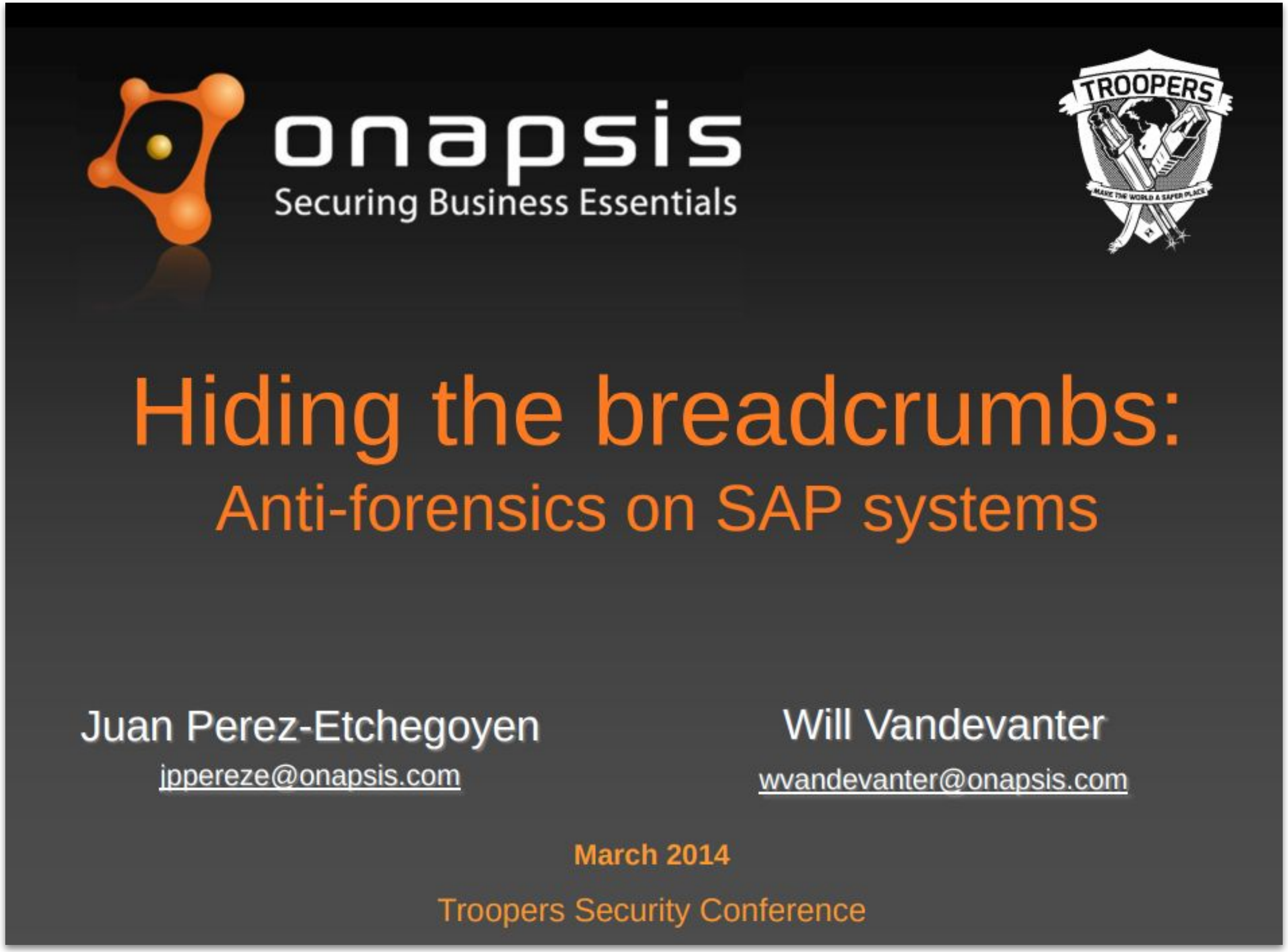
ERPScan

Dmitry Chastukhin
Evgeny Neyolov

Offensive talk with forensic and anti-forensic part at the end

https://www.youtube.com/watch?v=P9DleNshOa8

Why SAP Forensic ?



onapsis
Securing Business Essentials

Hiding the breadcrumbs:
Anti-forensics on SAP systems

Juan Perez-Etchegoyen
jppereze@onapsis.com

Will Vandevanter
wvandevanter@onapsis.com

March 2014

Troopers Security Conference

2014

Onapsis

Juan Perez-Etchegoyen
Will Vandevanter

Attack example and what was catch in logs (or not).

https://troopers.de/media/filer_public/14/60/1460e5ce-7a34-4dfc-8191-9da9f633f4ff/troopers14-hiding_the_breadcrumbs_anti-forensics_on_sap_systems-juanperez-etchegoyenwill_vandevanter.pdf

Why SAP Forensic ?

“Hard to cover this subject in 45 min talk”

Required different knowledge

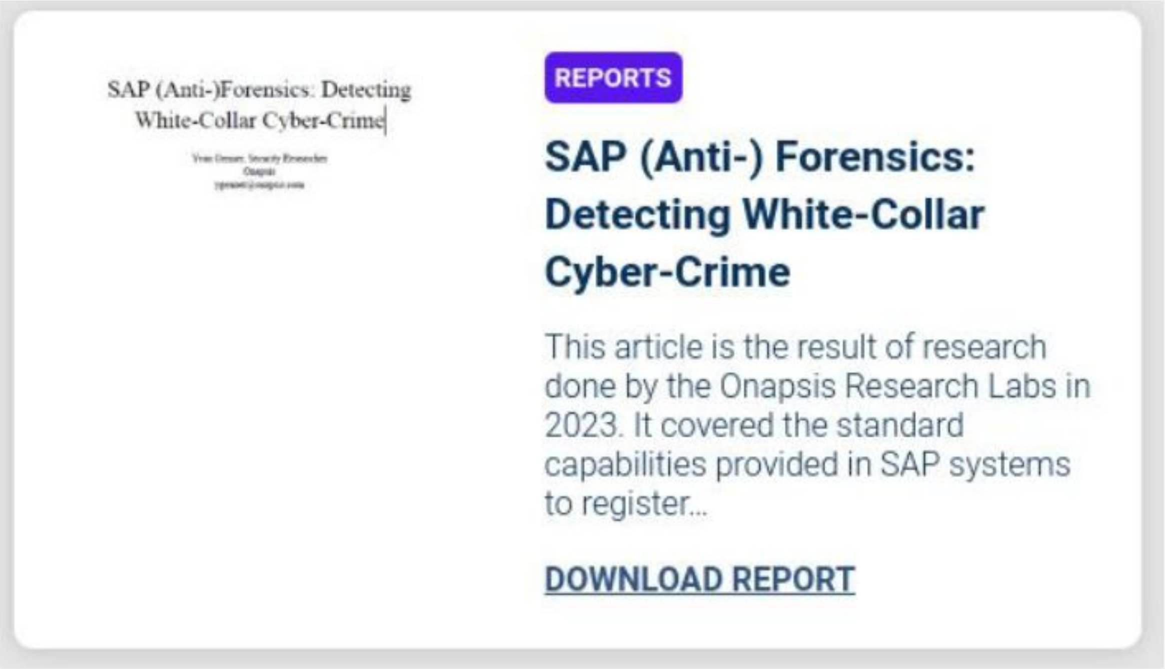
10 years old informations…
… a lot of things happened in SAP Security since

AGENDA

0x01	Why SAP Forensic ?
0x02	**The White Paper**
0x03	SAP Data Sources
0x04	Good to know…
0x05	Closing part

The White Paper

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

Yvan Genuer, Security Researcher
Onapsis
ygenuer@onapsis.com

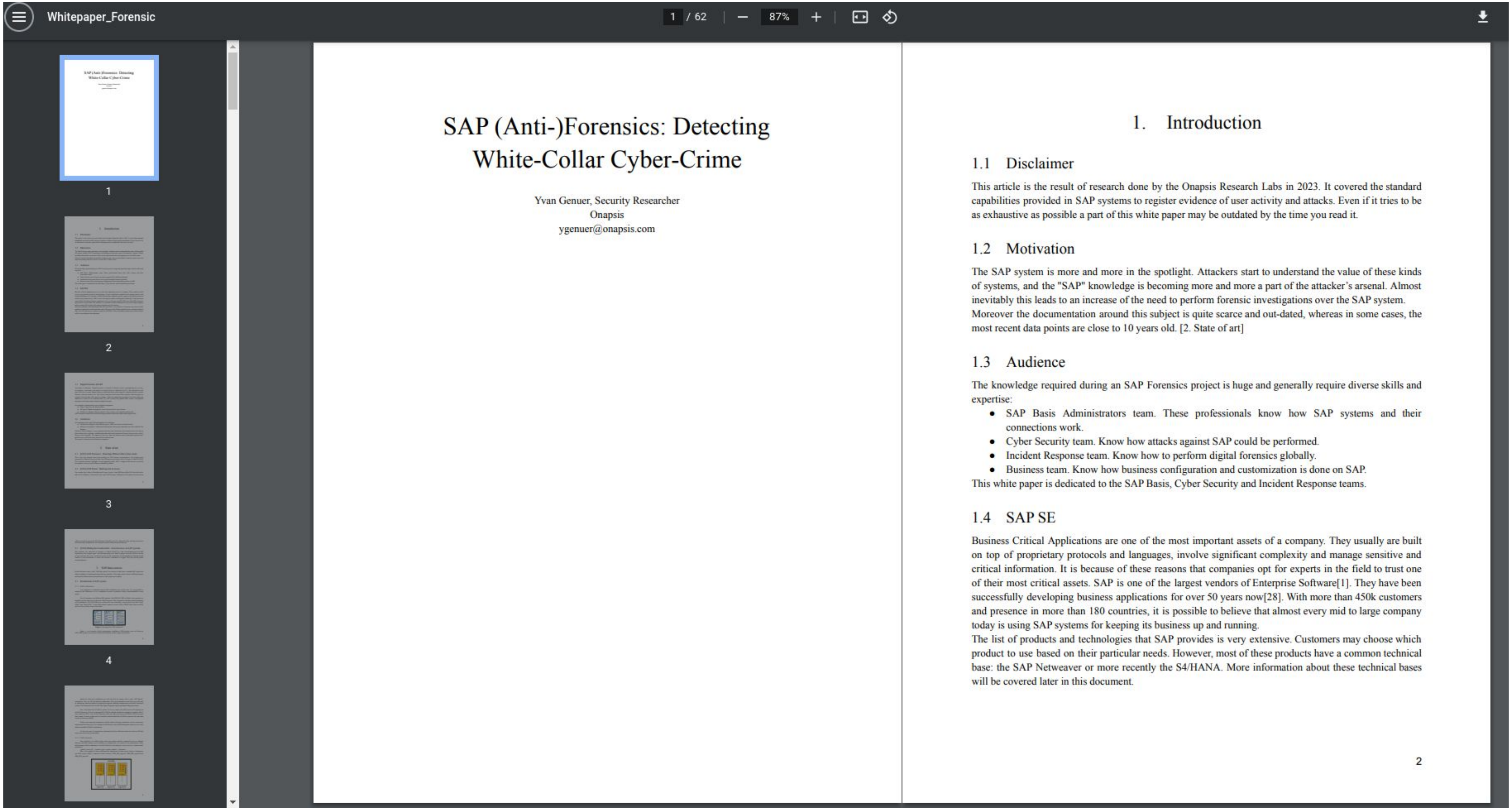
REPORTS

SAP (Anti-) Forensics: Detecting White-Collar Cyber-Crime

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard capabilities provided in SAP systems to register...

DOWNLOAD REPORT

The White Paper



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

Yvan Genuer, Security Researcher
Onapsis
ygenuer@onapsis.com

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard capabilities provided in SAP systems to register evidence of user activity and attacks. Even if it tries to be as exhaustive as possible a part of this white paper may be outdated by the time you read it.

1.2 Motivation

The SAP system is more and more in the spotlight. Attackers start to understand the value of these kinds of systems, and the "SAP" knowledge is becoming more and more a part of the attacker's arsenal. Almost inevitably this leads to an increase of the need to perform forensic investigations over the SAP system. Moreover the documentation around this subject is quite scarce and out-dated, whereas in some cases, the most recent data points are close to 10 years old. [2. State of art]

1.3 Audience

The knowledge required during an SAP Forensics project is huge and generally require diverse skills and expertise:

- SAP Basis Administrators team. These professionals know how SAP systems and their connections work.
- Cyber Security team. Know how attacks against SAP could be performed.
- Incident Response team. Know how to perform digital forensics globally.
- Business team. Know how business configuration and customization is done on SAP.

This white paper is dedicated to the SAP Basis, Cyber Security and Incident Response teams.

1.4 SAP SE

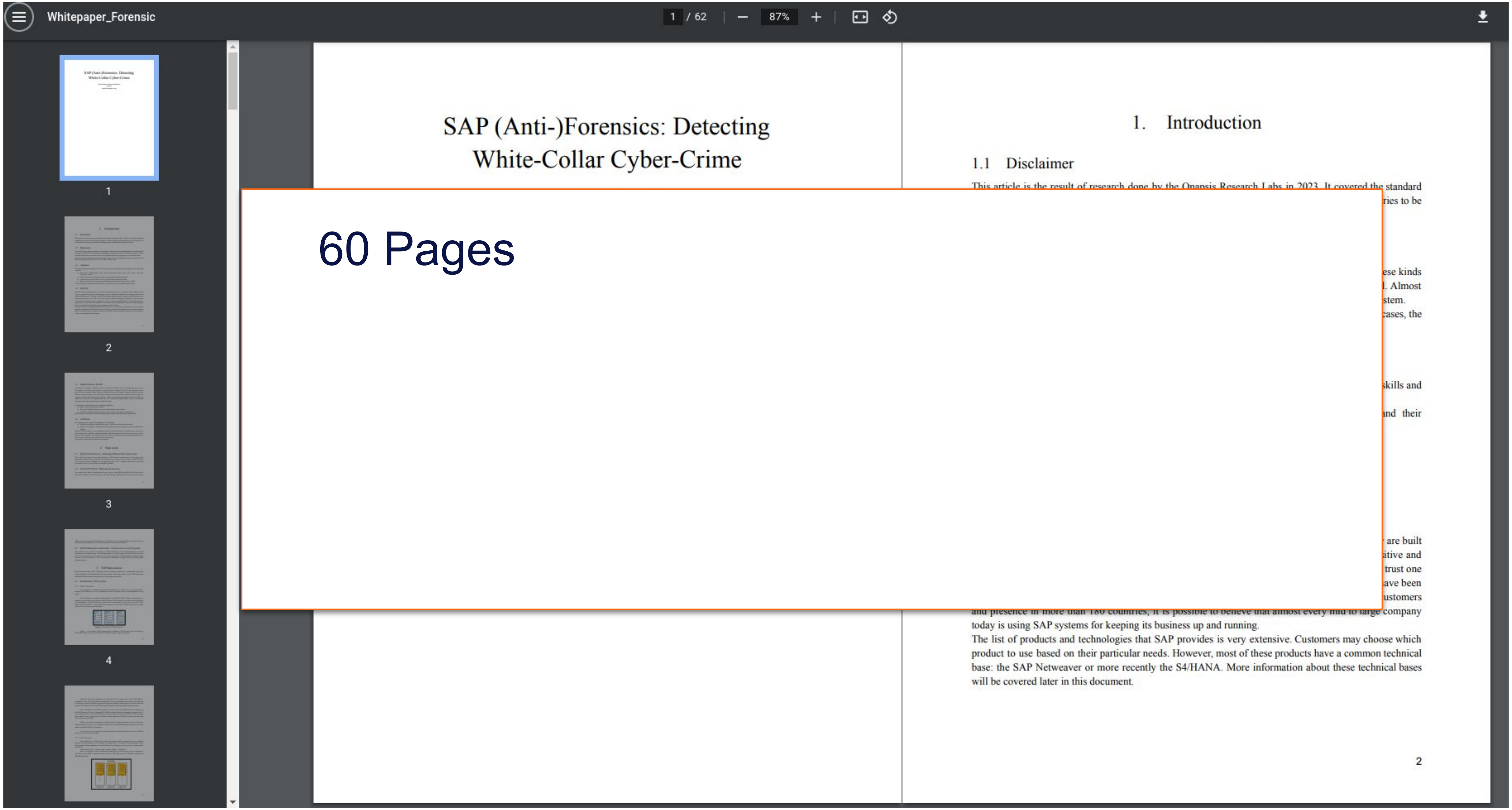
Business Critical Applications are one of the most important assets of a company. They usually are built on top of proprietary protocols and languages, involve significant complexity and manage sensitive and critical information. It is because of these reasons that companies opt for experts in the field to trust one of their most critical assets. SAP is one of the largest vendors of Enterprise Software[1]. They have been successfully developing business applications for over 50 years now[28]. With more than 450k customers and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.

The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

The White Paper



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard

ries to be

ese kinds

l. Almost

stem.

cases, the

skills and

and their

are built

itive and

trust one

ave been

ustomers

and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.

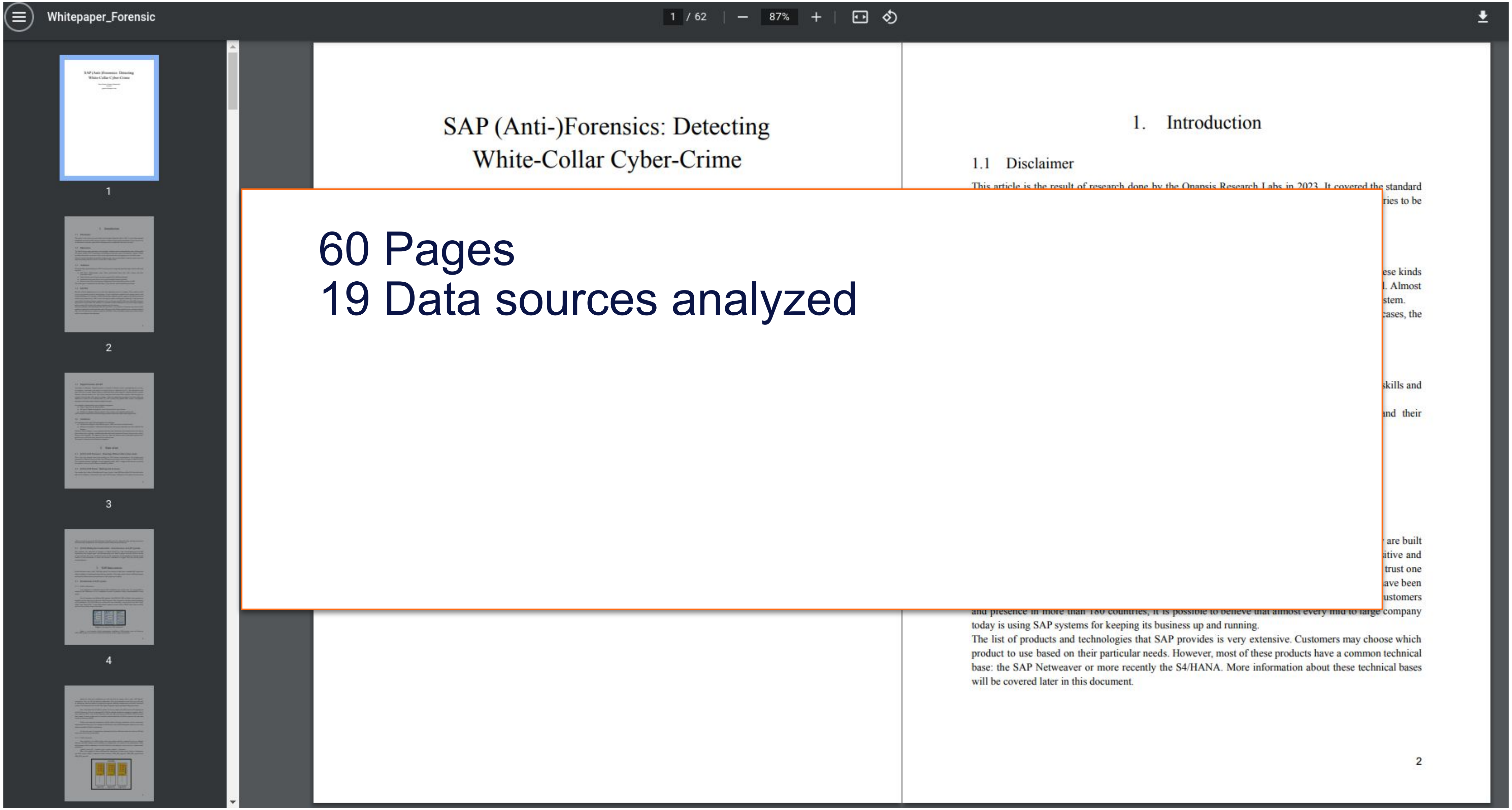
The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

60 Pages

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

The White Paper



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard
ries to be

ese kinds
l. Almost
stem.
cases, the

skills and

and their

are built
itive and
trust one
ave been
ustomers
and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.

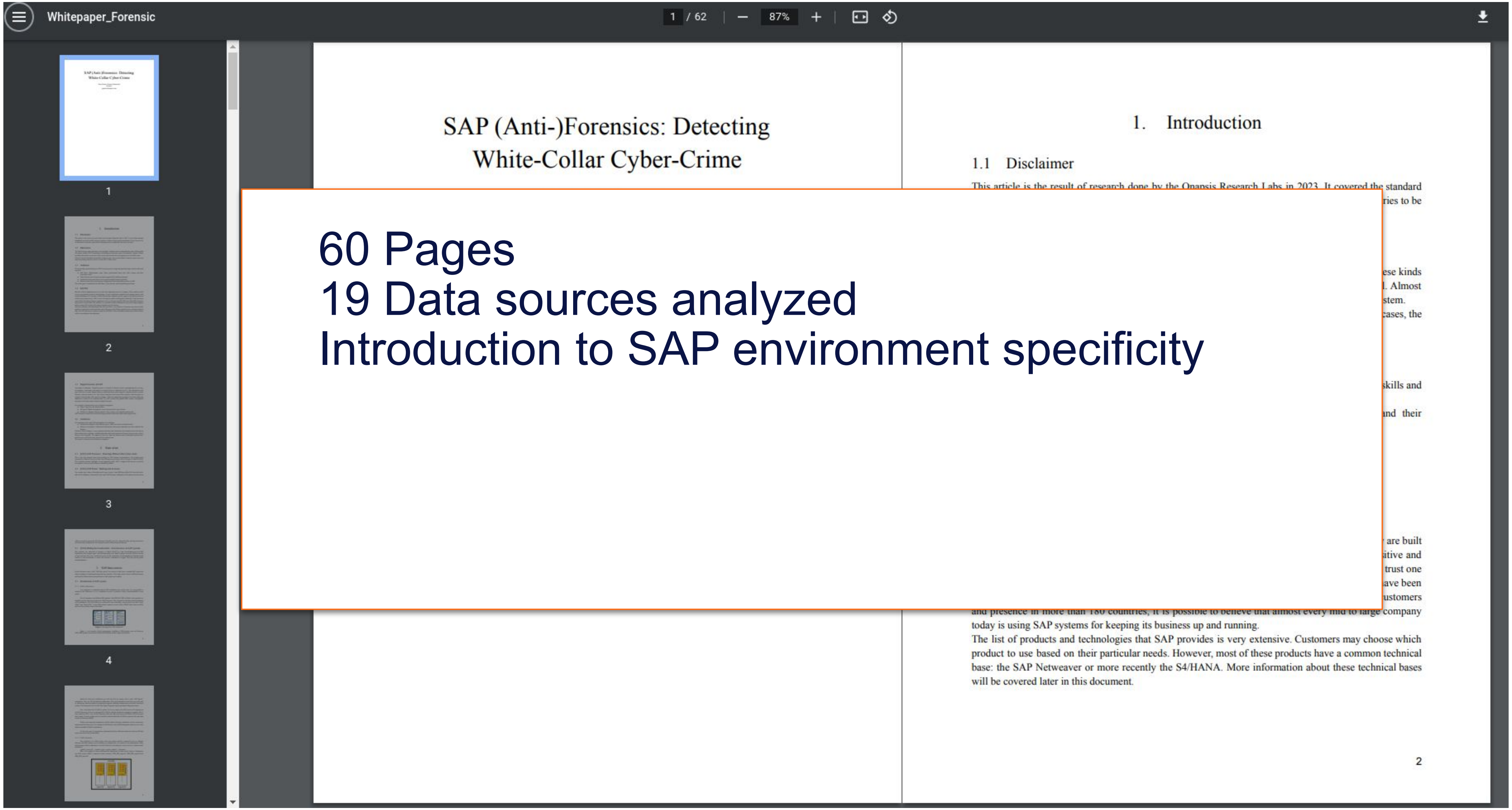
The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

60 Pages
19 Data sources analyzed

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

The White Paper



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard
ries to be

ese kinds
l. Almost
stem.
cases, the

skills and

and their

are built
itive and
trust one
ave been
ustomers
and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.

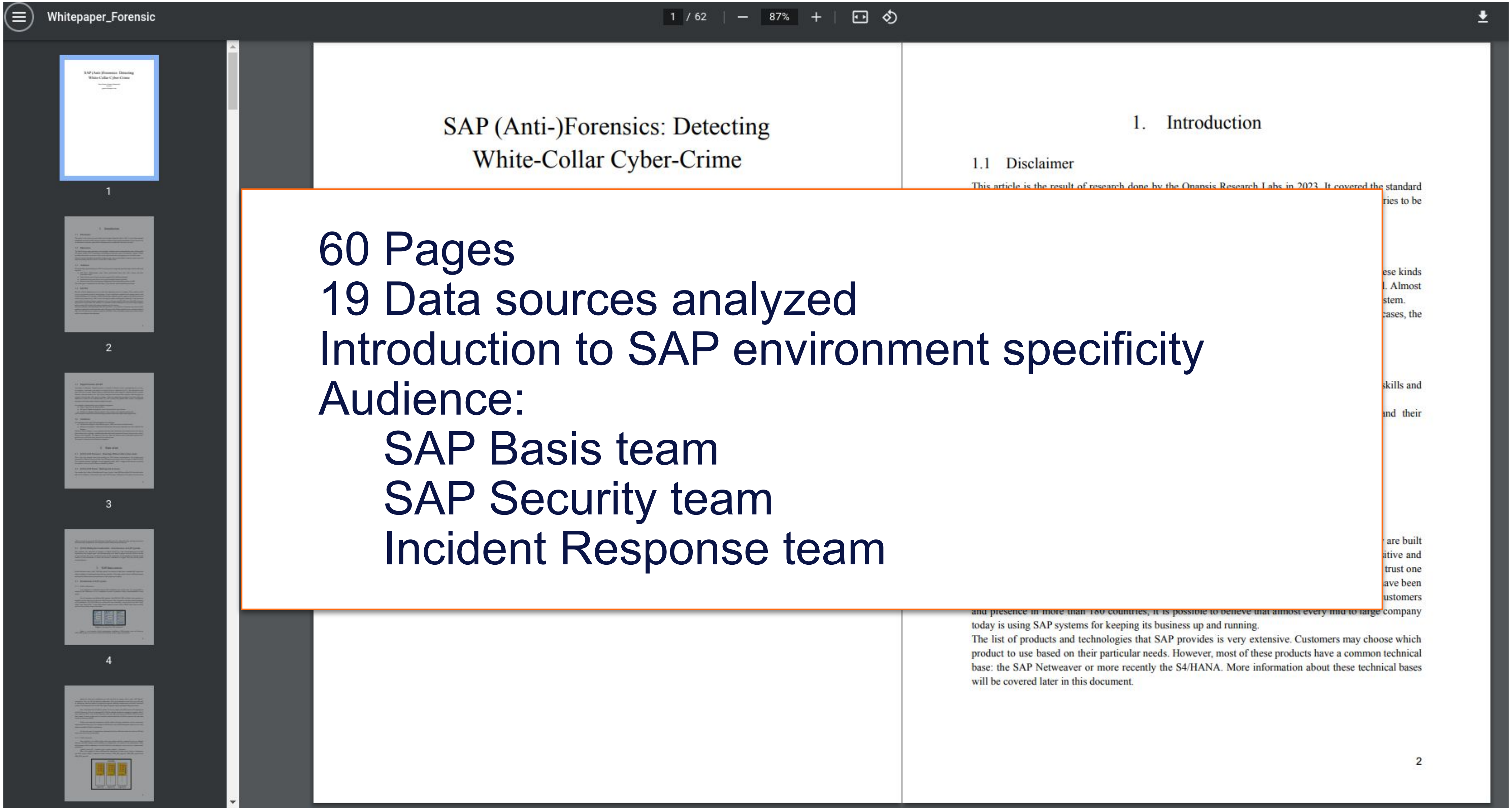
The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

60 Pages
19 Data sources analyzed
Introduction to SAP environment specificity

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

The White Paper



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard

ries to be

ese kinds

l. Almost

stem.

cases, the

skills and

and their

are built

sitive and

trust one

ave been

ustomers

and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.

The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

60 Pages
19 Data sources analyzed
Introduction to SAP environment specificity
Audience:

- SAP Basis team
- SAP Security team
- Incident Response team

https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

The White Paper

Technical Investigation

How attackers get in and navigate ? Which services was accessed ? What was added, modified or deleted ?

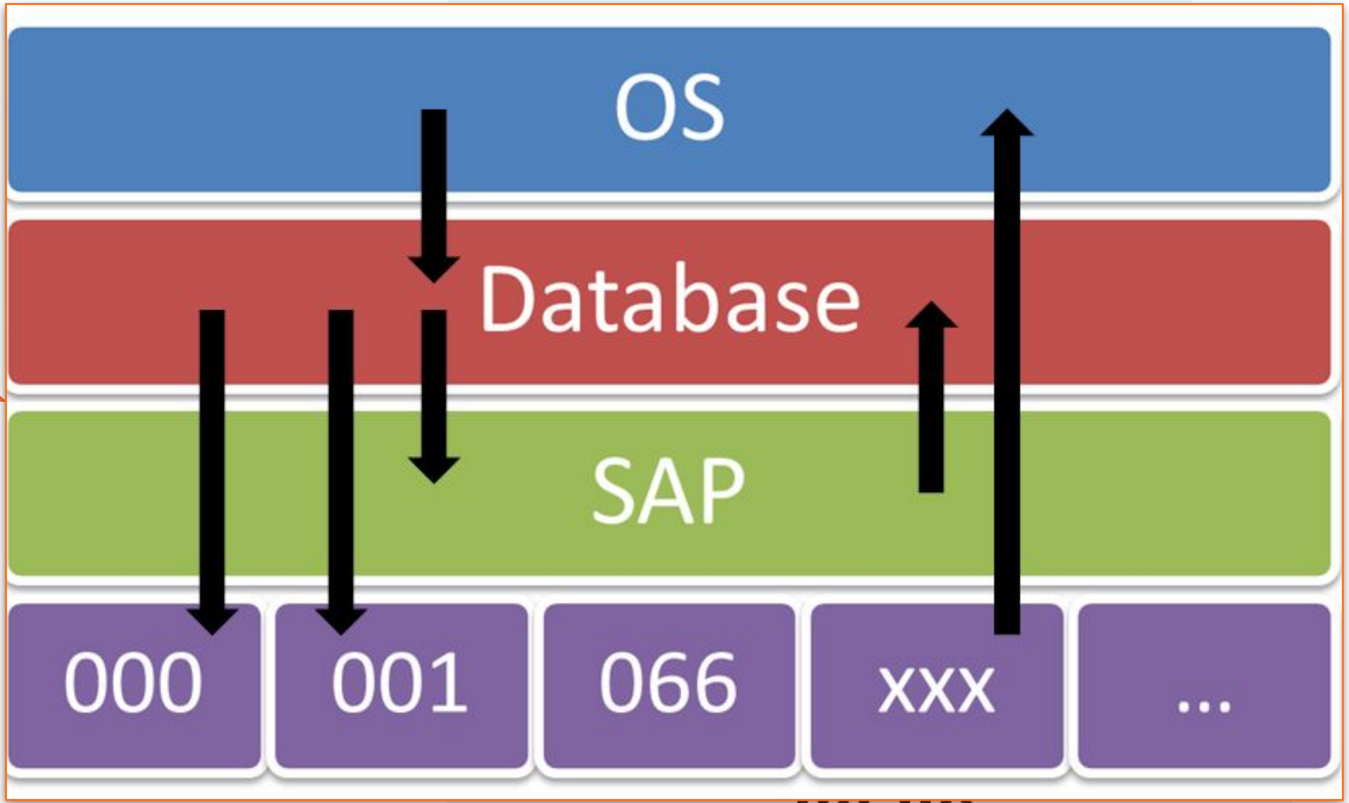
Business Investigation

What attackers did as post exploitation activities related to the business ?

The White Paper

Technical Investigation

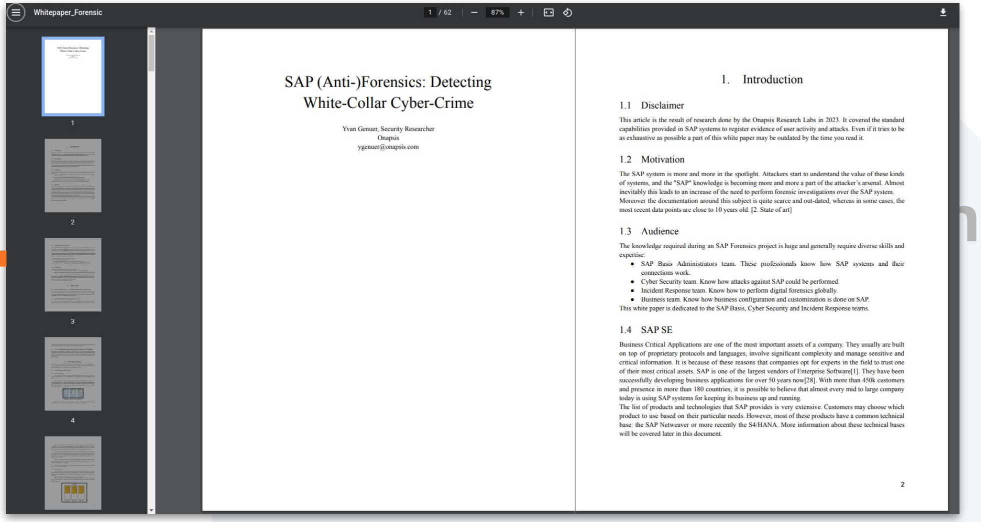
How attackers get in and navigate ? Which services was accessed ? What was added, modified or deleted ?



The White Paper

Technical Investigation

How attackers get in and navigate ? Which services was accessed ? What was added, modified or deleted ?



SAP (Anti-)Forensics: Detecting White-Collar Cyber-Crime

Yvan Genuer, Security Researcher
Onapsis
ygenuer@onapsis.com

1. Introduction

1.1 Disclaimer

This article is the result of research done by the Onapsis Research Labs in 2023. It covered the standard capabilities provided in SAP systems to register evidence of user activity and attacks. Even if it tries to be as exhaustive as possible a part of this white paper may be outdated by the time you read it.

1.2 Motivation

The SAP system is more and more in the spotlight. Attackers start to understand the value of these kinds of systems, and the "SAP" knowledge is becoming more and more a part of the attacker's arsenal. Almost inevitably this leads to an increase of the need to perform forensic investigations over the SAP system. Moreover the documentation around this subject is quite scarce and out-dated, whereas in some cases, the most recent data points are close to 10 years old. [2. State of art]

1.3 Audience

The knowledge required during an SAP Forensics project is huge and generally require diverse skills and expertise:

- SAP Basis Administrators team. These professionals know how SAP systems and their connections work.
- Cyber Security team. Know how attacks against SAP could be performed.
- Incident Response team. Know how to perform digital forensics globally.
- Business team. Know how business configuration and customization is done on SAP.

This white paper is dedicated to the SAP Basis, Cyber Security and Incident Response teams.

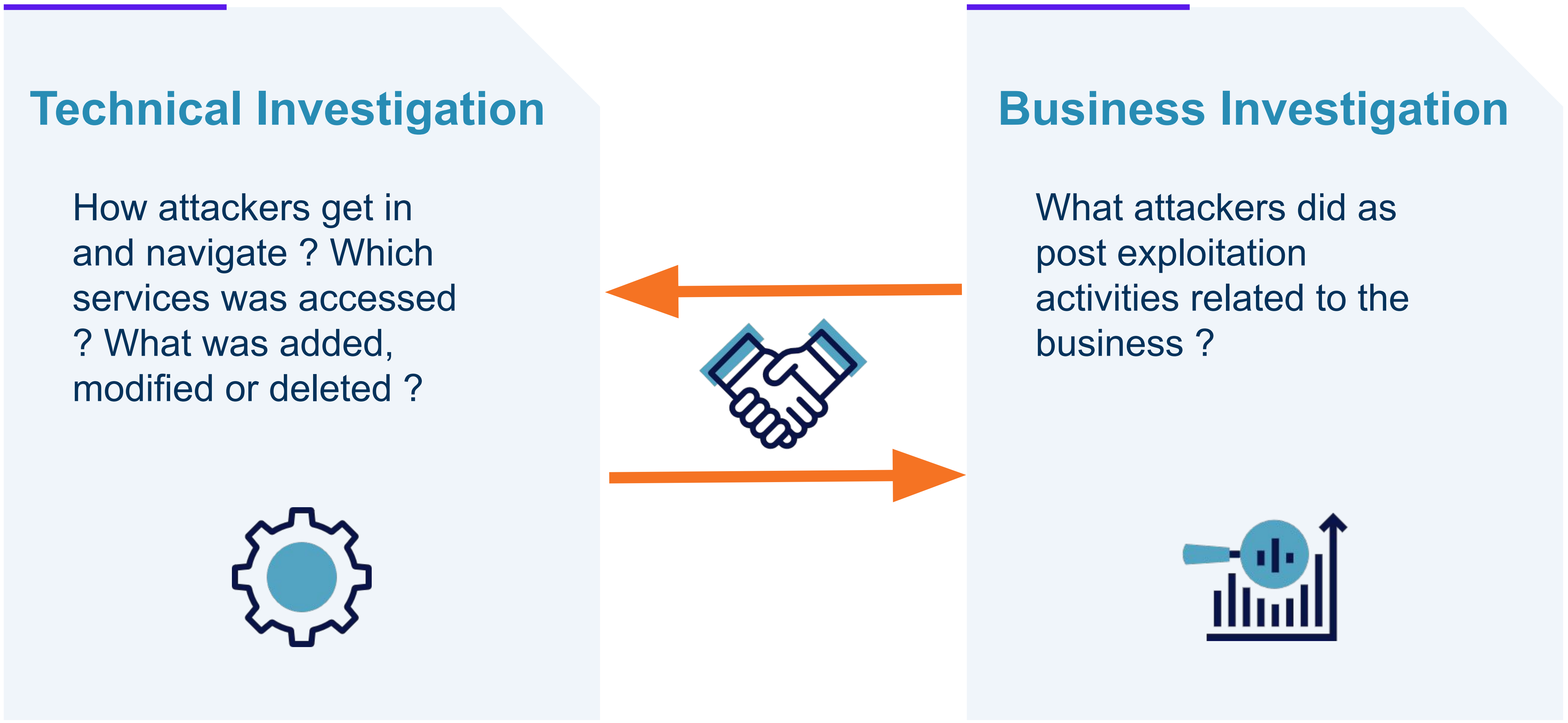
1.4 SAP SE

Business Critical Applications are one of the most important assets of a company. They usually are built on top of proprietary protocols and languages, involve significant complexity and manage sensitive and critical information. It is because of these reasons that companies opt for experts in the field to trust one of their most critical assets. SAP is one of the largest vendors of Enterprise Software[1]. They have been successfully developing business applications for over 50 years now[28]. With more than 450k customers and presence in more than 180 countries, it is possible to believe that almost every mid to large company today is using SAP systems for keeping its business up and running.
The list of products and technologies that SAP provides is very extensive. Customers may choose which product to use based on their particular needs. However, most of these products have a common technical base: the SAP Netweaver or more recently the S4/HANA. More information about these technical bases will be covered later in this document.

2

business ?

The White Paper



Technical Investigation

How attackers get in and navigate ? Which services was accessed ? What was added, modified or deleted ?

Business Investigation

What attackers did as post exploitation activities related to the business ?

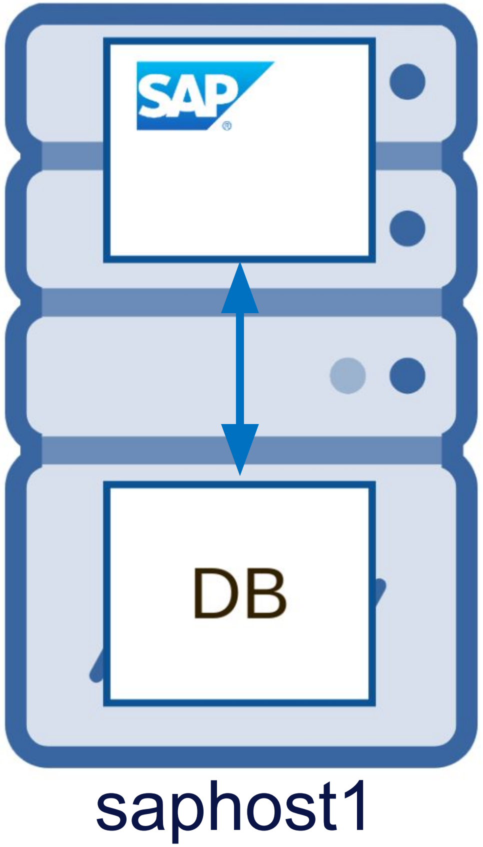
AGENDA

0x01	Why SAP Forensic ?
0x02	The White Paper
0x03	**SAP Data Sources**
0x04	Good to know…
0x05	Closing part

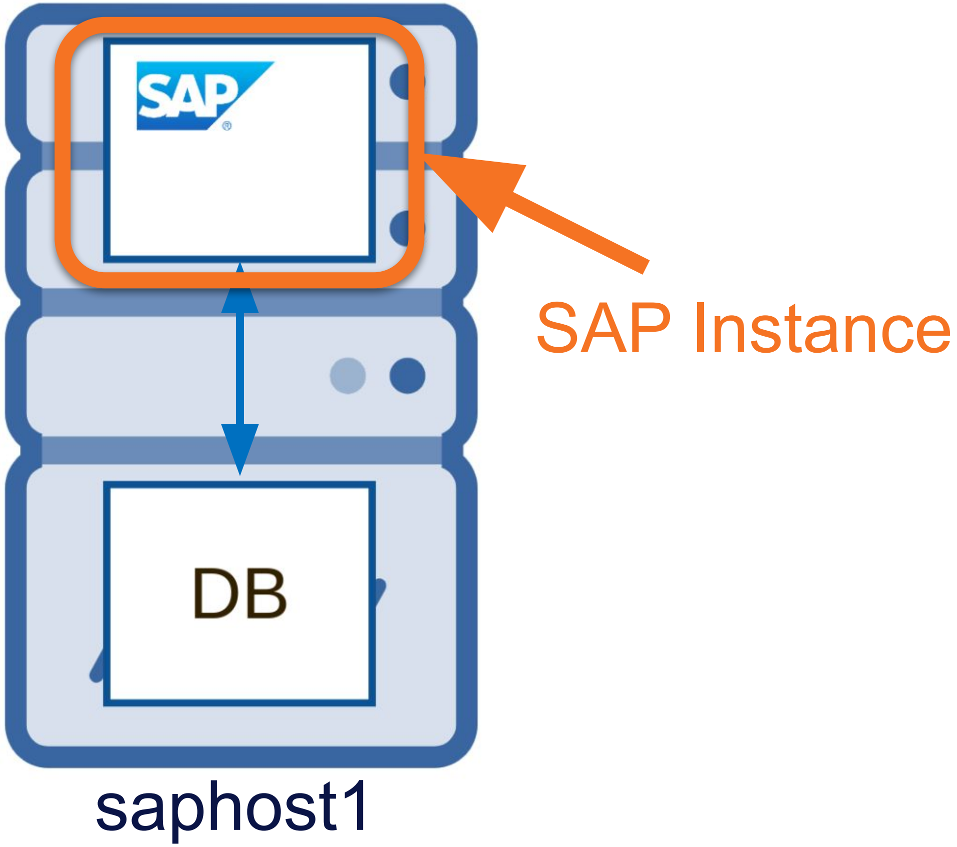
SAP Data Sources

> *“SAP data sources” are sources of data from a standard SAP system that help investigators to understand usage and trace intruders.*

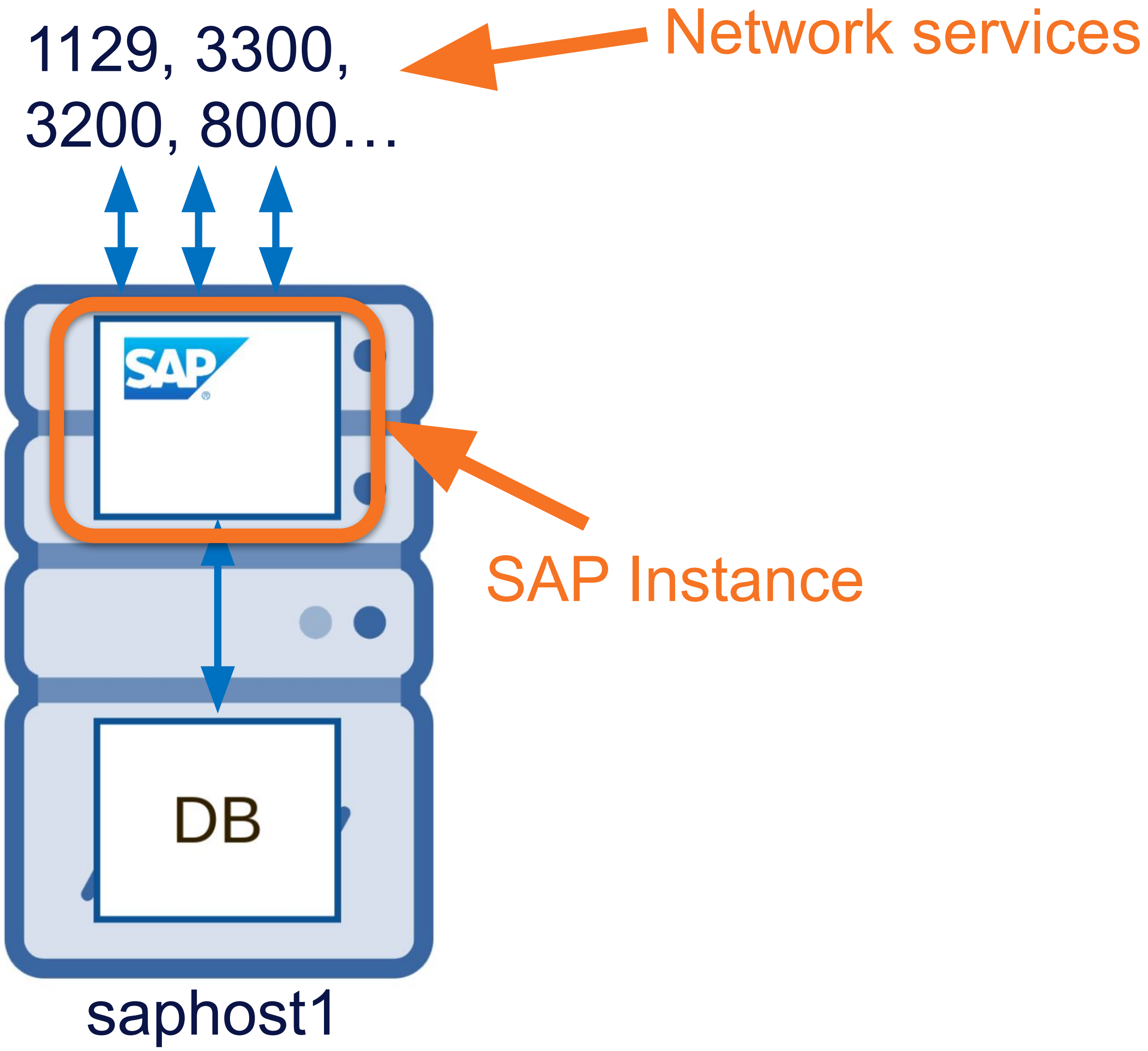
SAP Data Sources



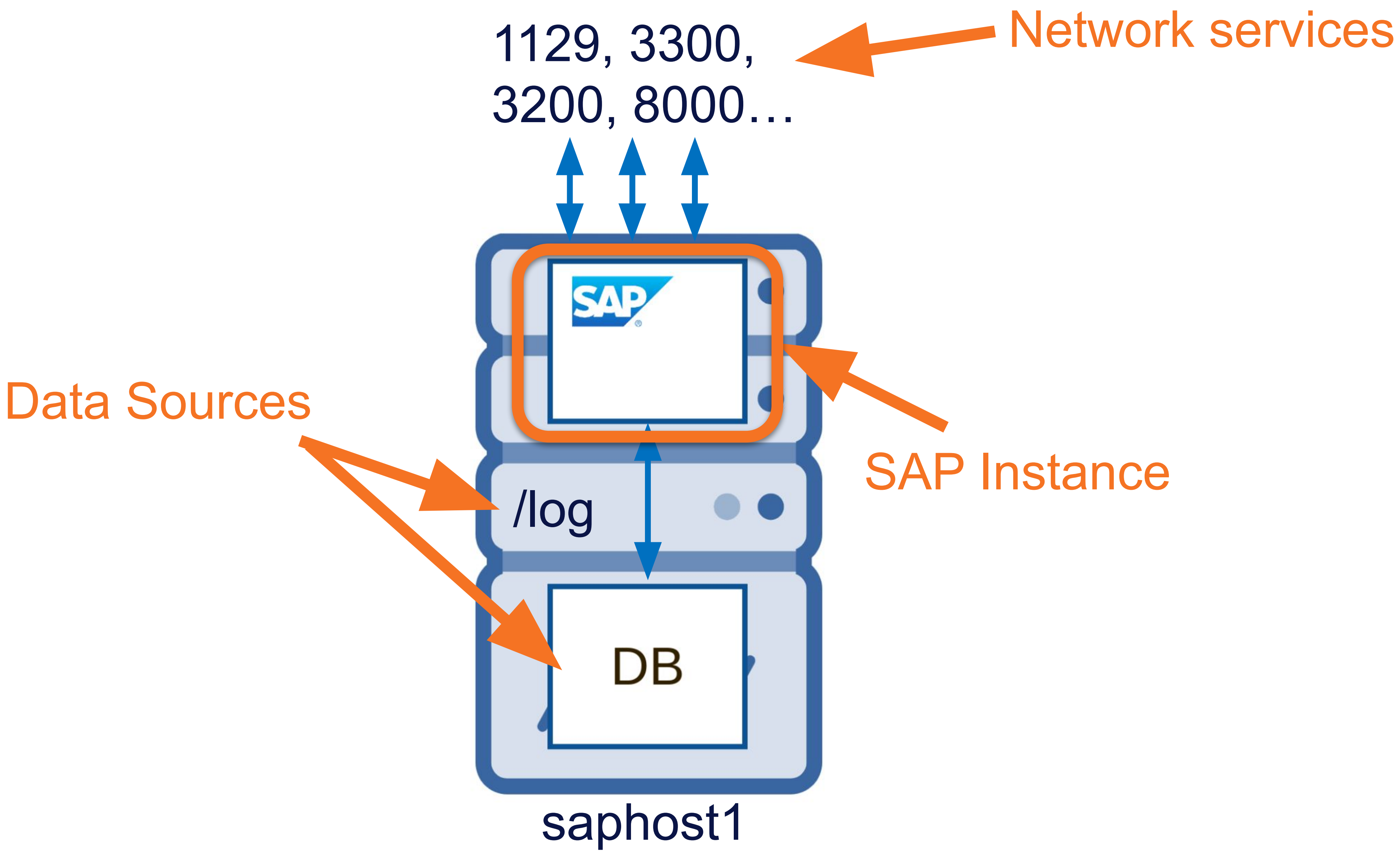
SAP Data Sources



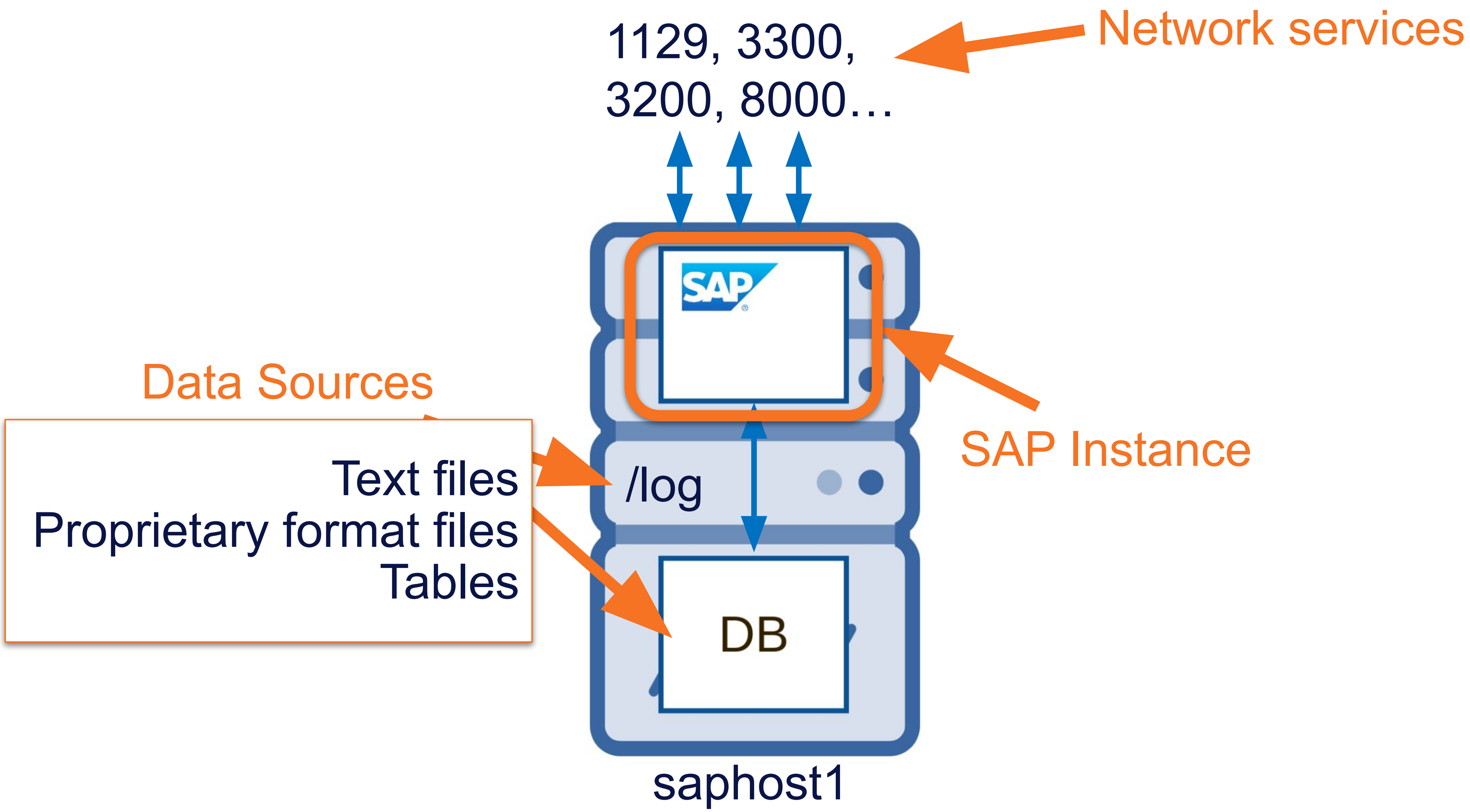
SAP Data Sources



SAP Data Sources



SAP Data Sources



Network services

1129, 3300,
3200, 8000…

SAP Instance

Data Sources

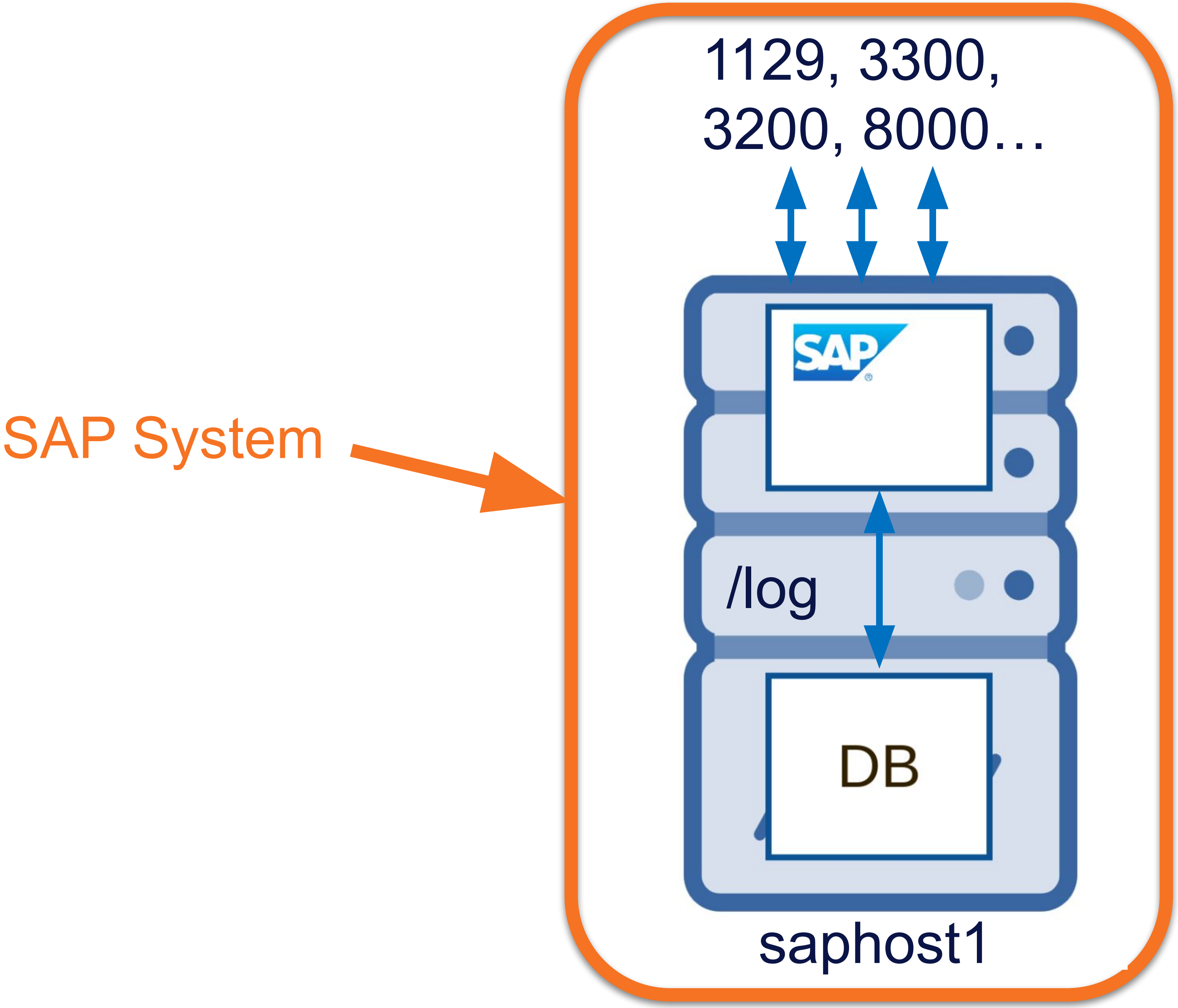
Text files
Proprietary format files
Tables

/log

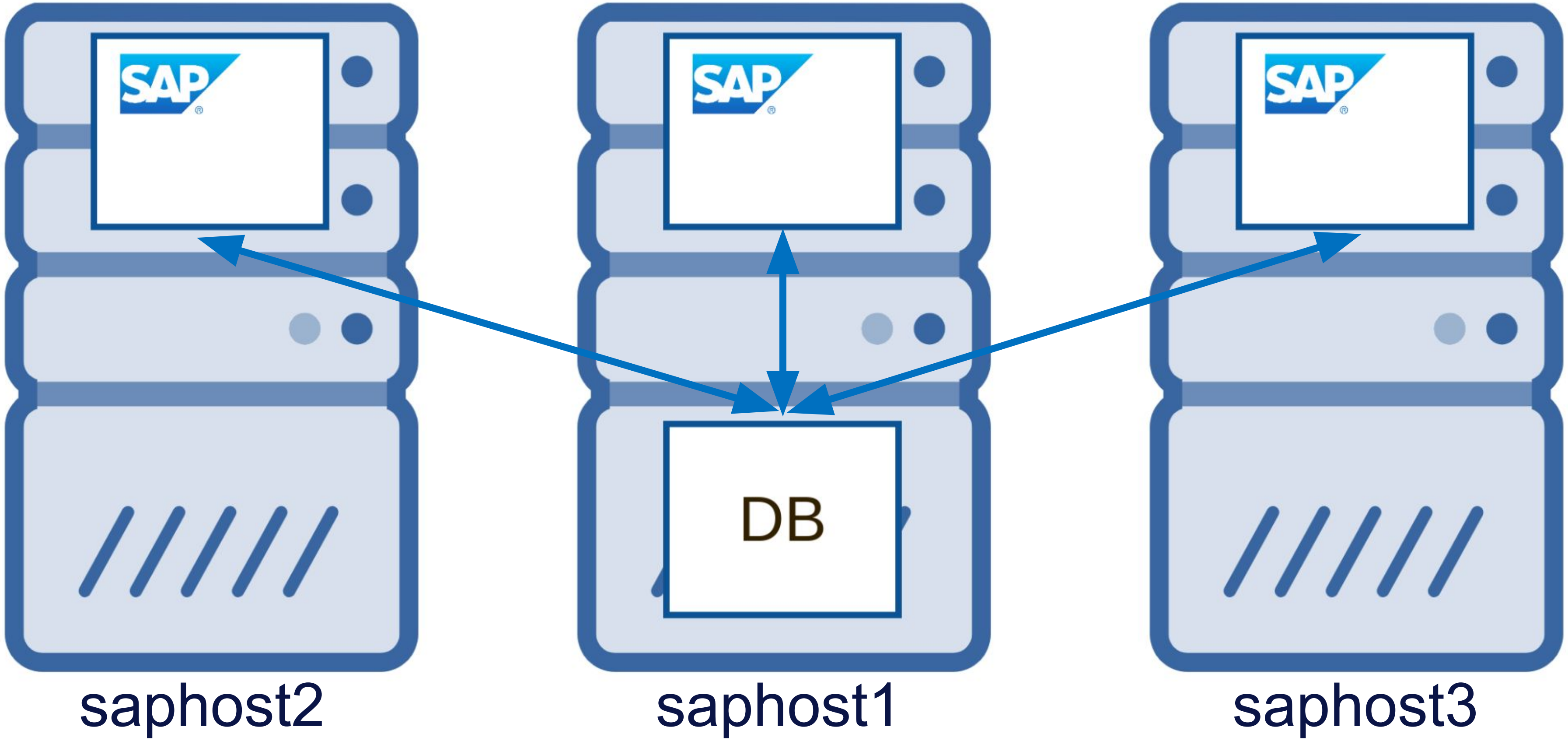
DB

saphost1

SAP Data Sources

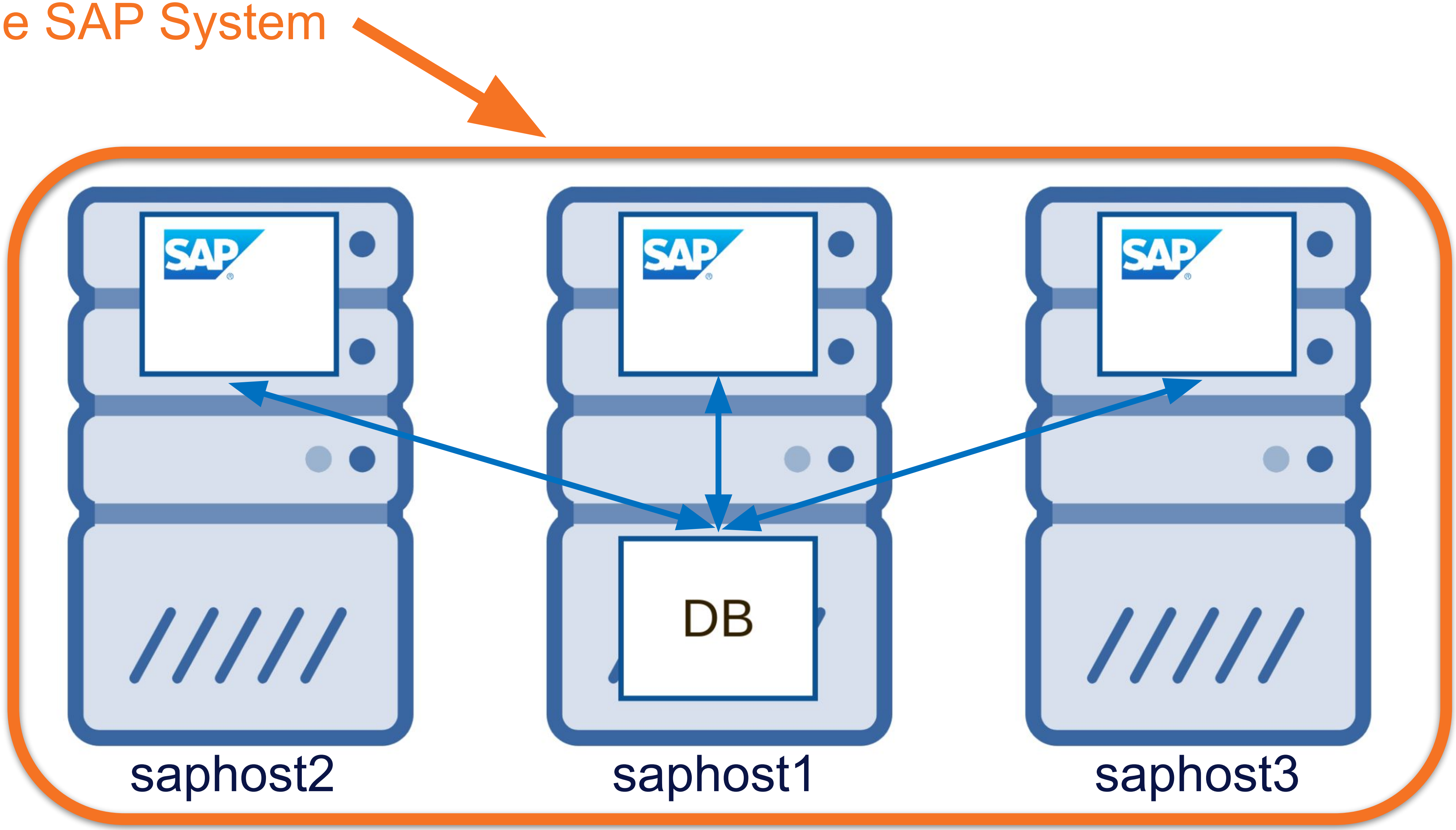


SAP Data Sources

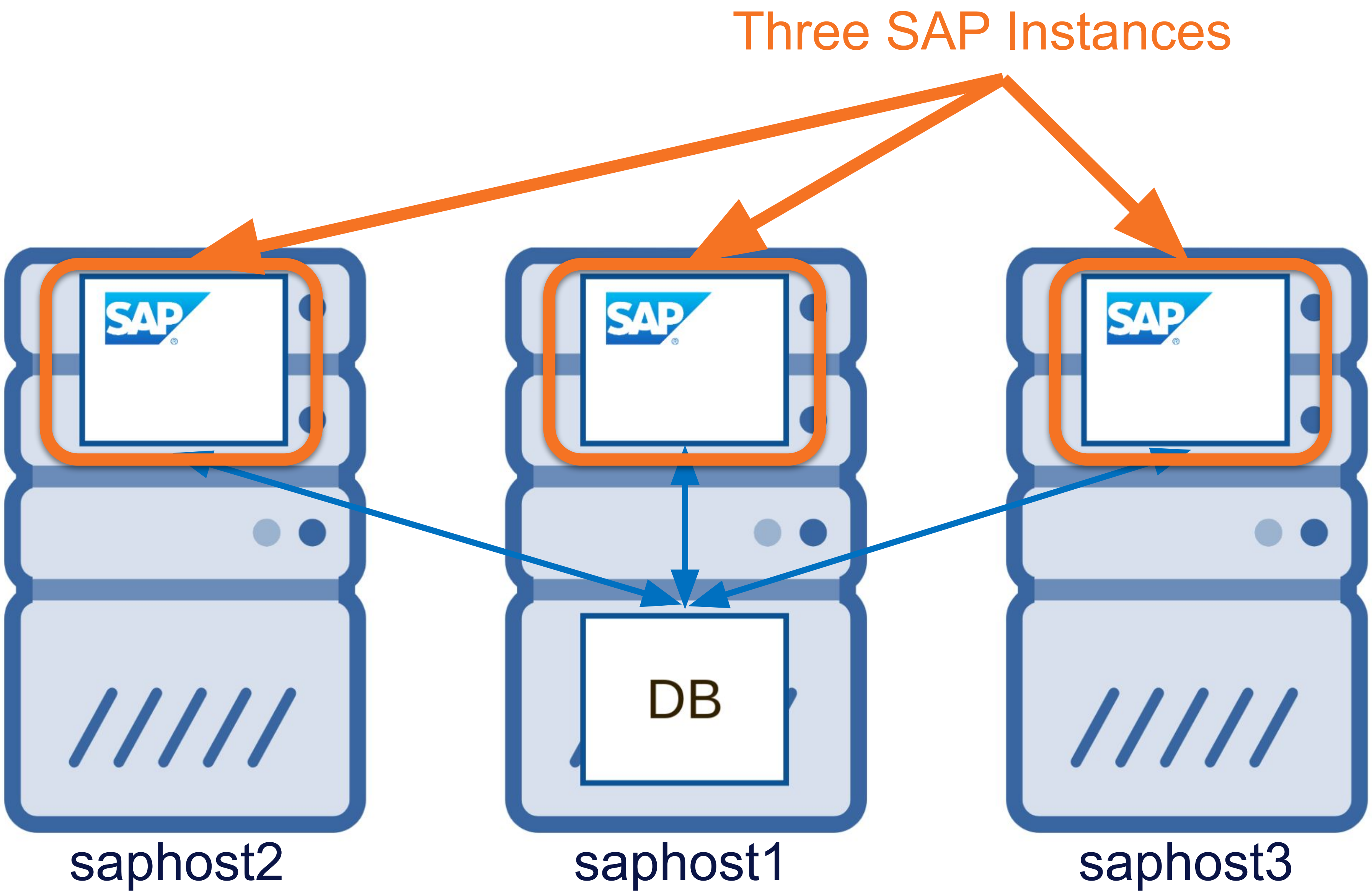


SAP Data Sources

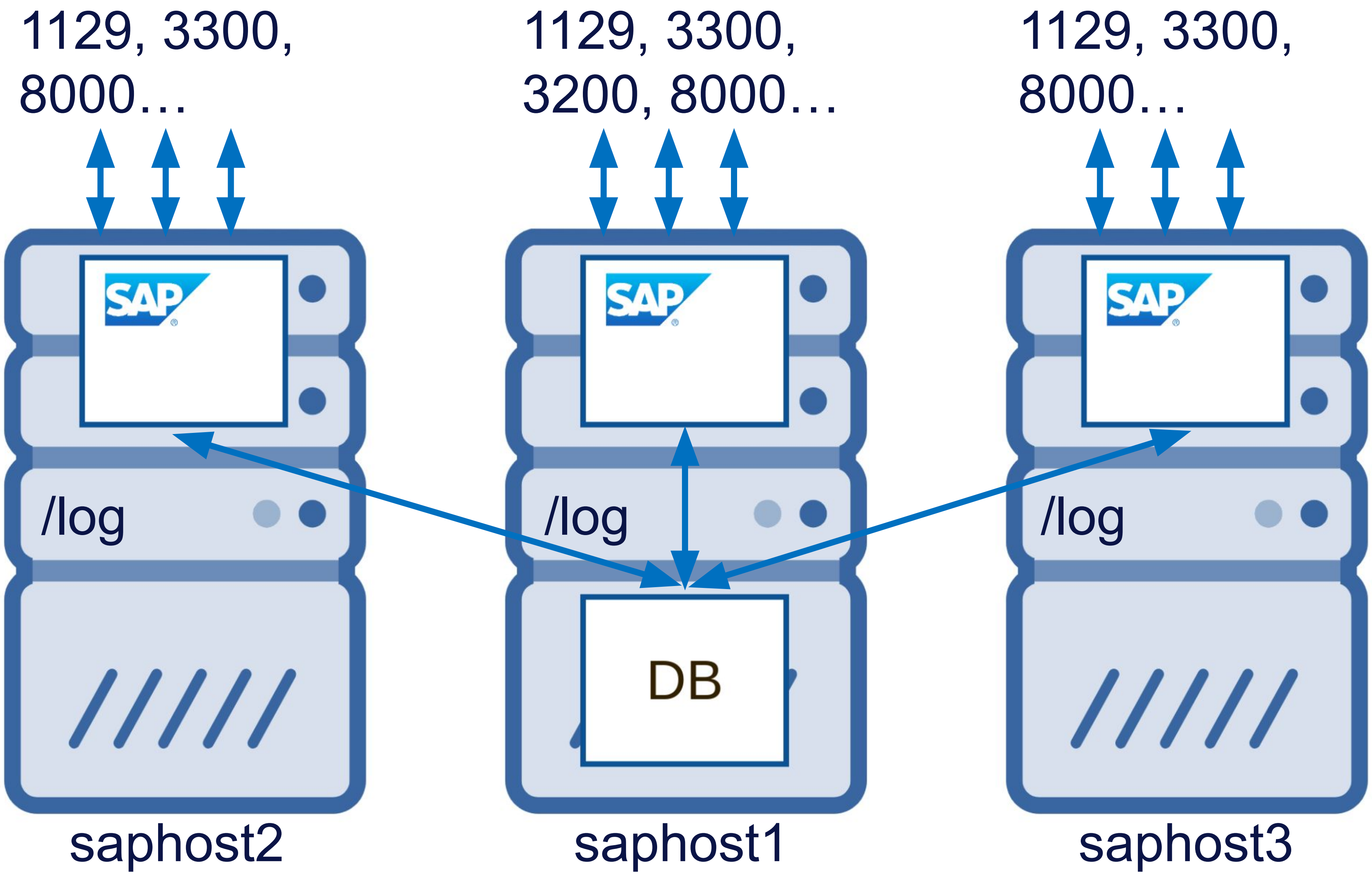
One SAP System



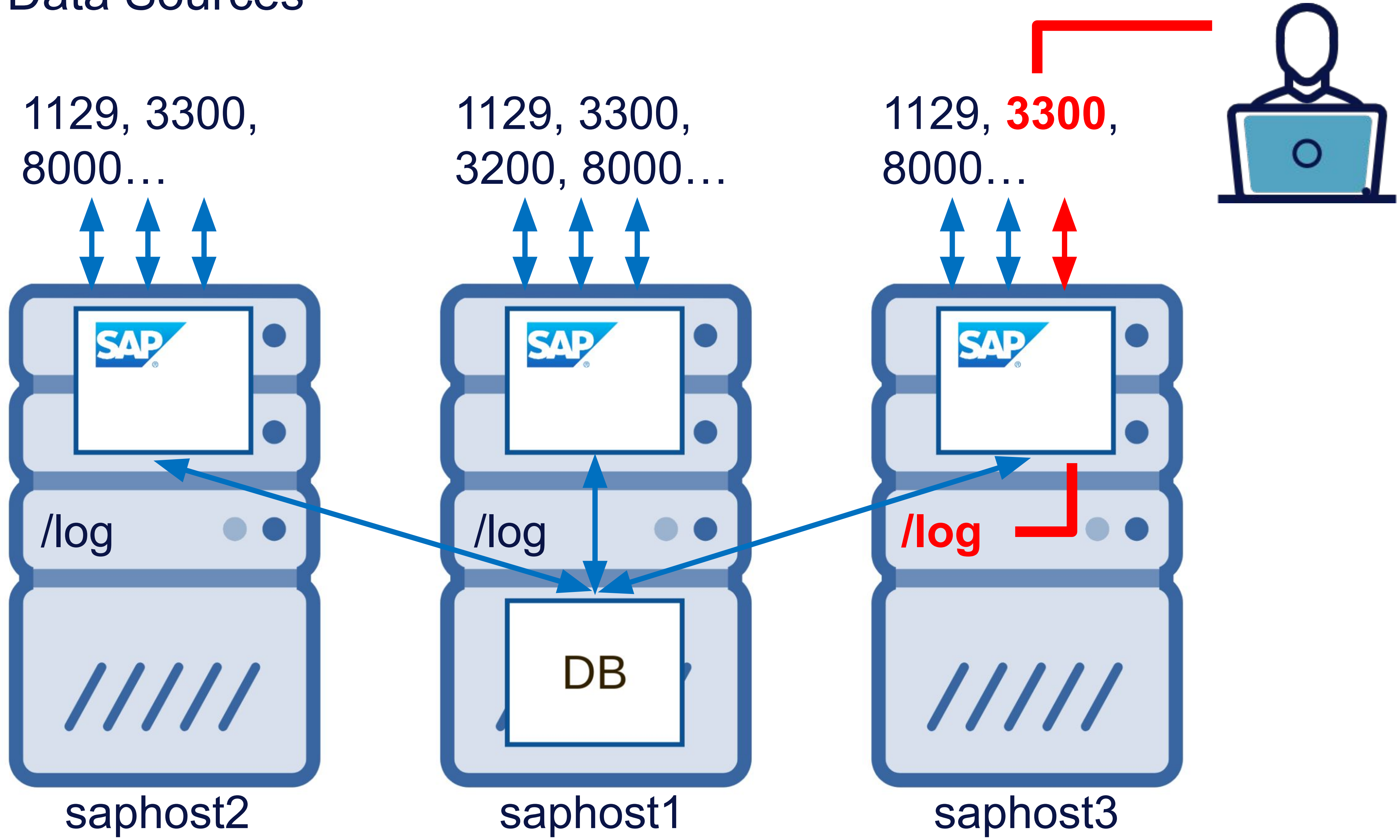
SAP Data Sources



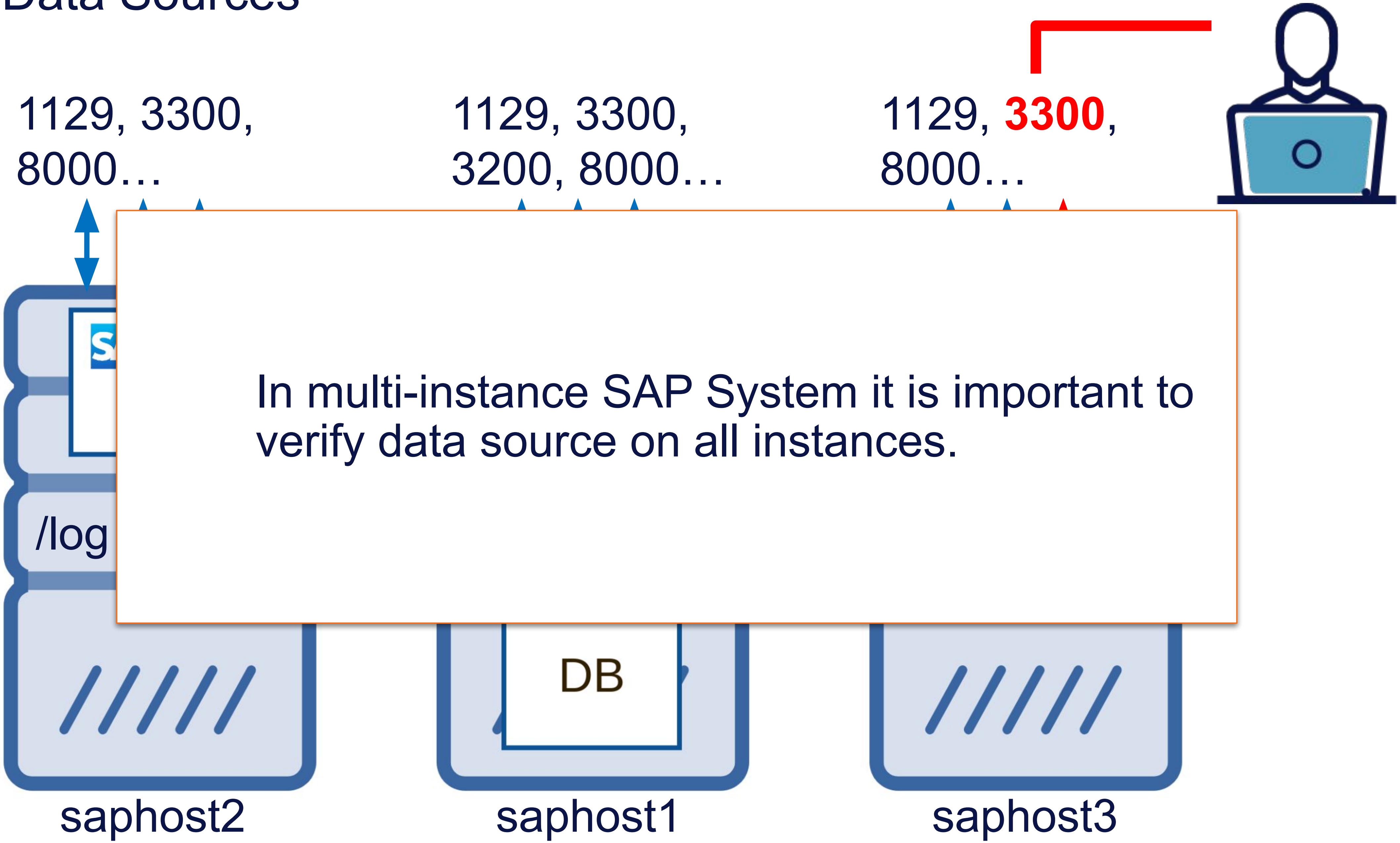
SAP Data Sources



SAP Data Sources



SAP Data Sources



In multi-instance SAP System it is important to verify data source on all instances.

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

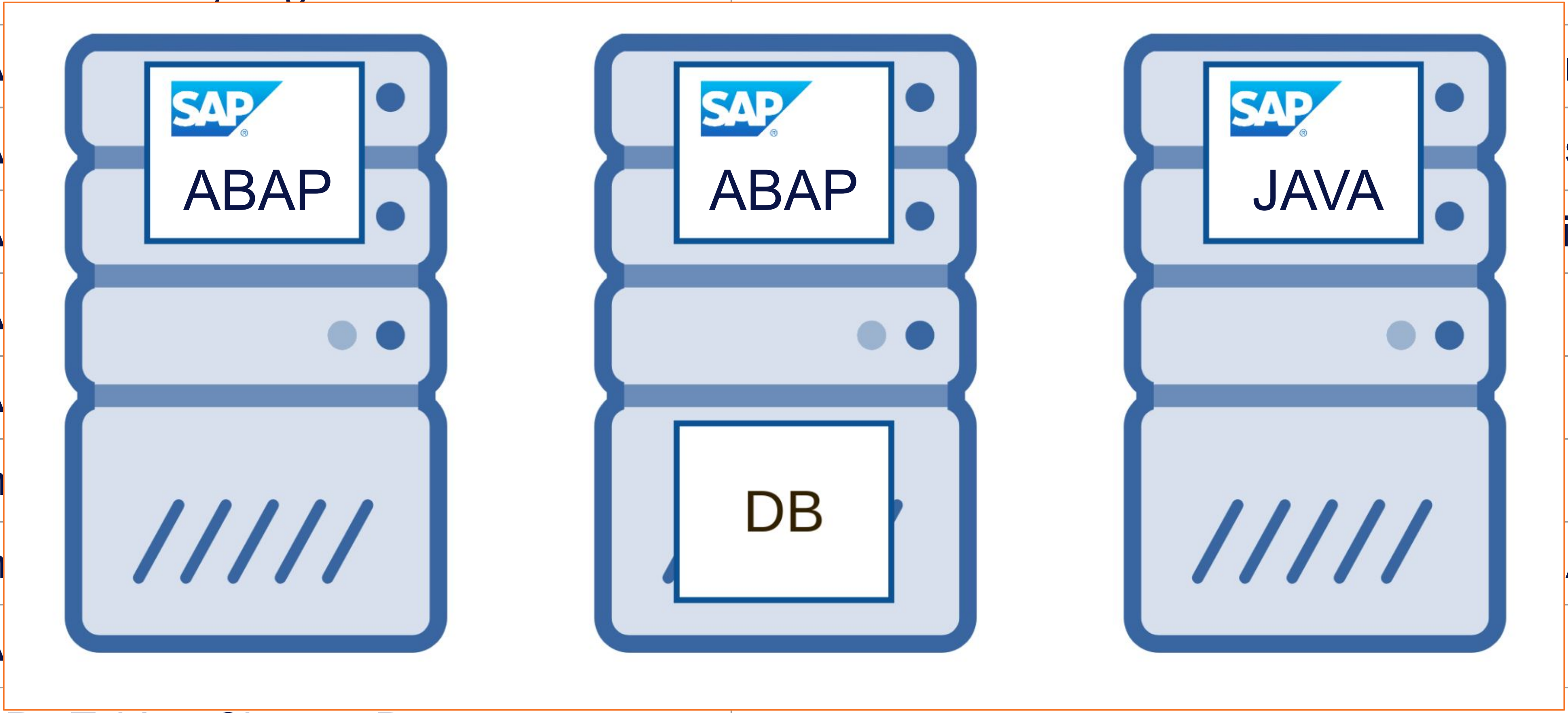
SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP -	
ABAP/J	
ABAP/J	
ABAP/J	
Standal	
Standal	log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

[SAP Instance Type] - [Source Type] - [Name]

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABA	ments
ABA	s
ABA	ice
ABA	
ABA	
Stan	
Stan	Agent log
ABA	
ABAP - Table - Change Documents	



SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

SAP Data Sources

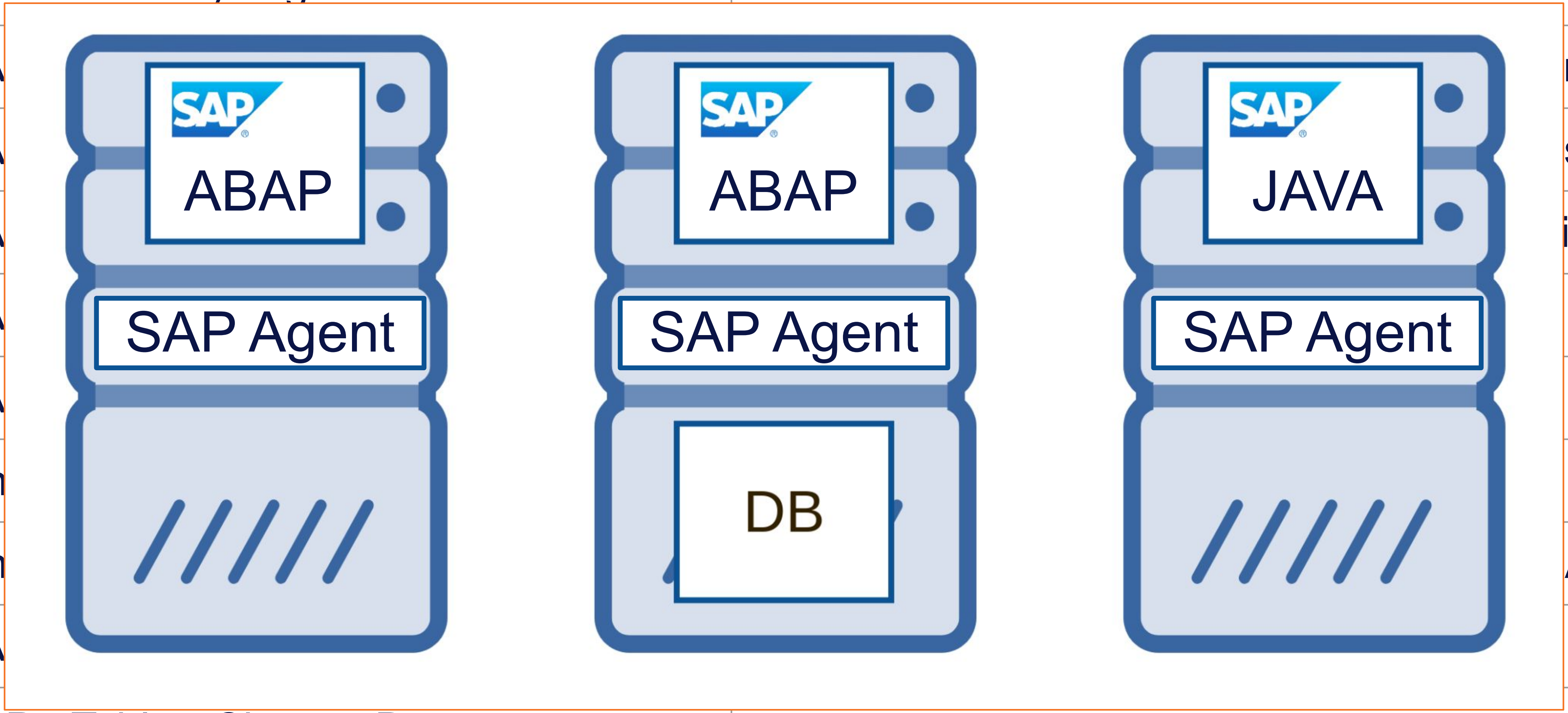
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/**JAVA** - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/**JAVA** - File - Gateway	ABAP/**JAVA** - File - Internet Graphical Service
ABAP/**JAVA** - File - Message Server	ABAP - Table - System Traces
ABAP/**JAVA** - File - ICM Service	**JAVA** - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	**Agent** - File - Start Service log
Standalone - File - SAPRouter Log	**Agent** - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	**Agent** - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABA	ments
ABA	s
ABA	ice
ABA	
ABA	
Stan	
Stan	Agent log
ABA	
ABAP - Table - Change Documents	



SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

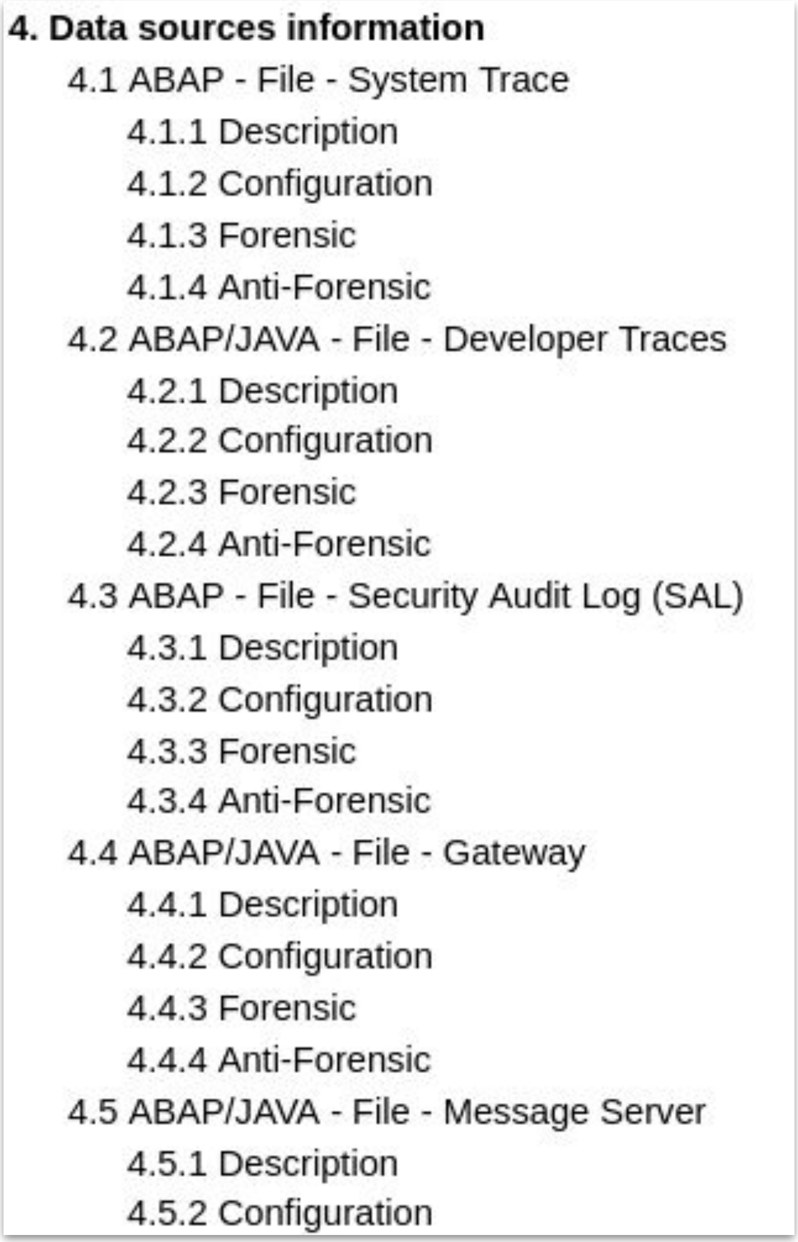
SAP Data Sources

ABAP - **File** - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - **File** - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - **File** - Security Audit Log	ABAP - **File** - Business Transaction Analysis
ABAP/JAVA - **File** - Gateway	ABAP/JAVA - **File** - Internet Graphical Service
ABAP/JAVA - **File** - Message Server	ABAP - Table - System Traces
ABAP/JAVA - **File** - ICM Service	JAVA - **File** - Log Viewer
Standalone - **File** - Web Dispatcher	Agent - **File** - Start Service log
Standalone - **File** - SAPRouter Log	Agent - **File** - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - **File** - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

SAP Data Sources

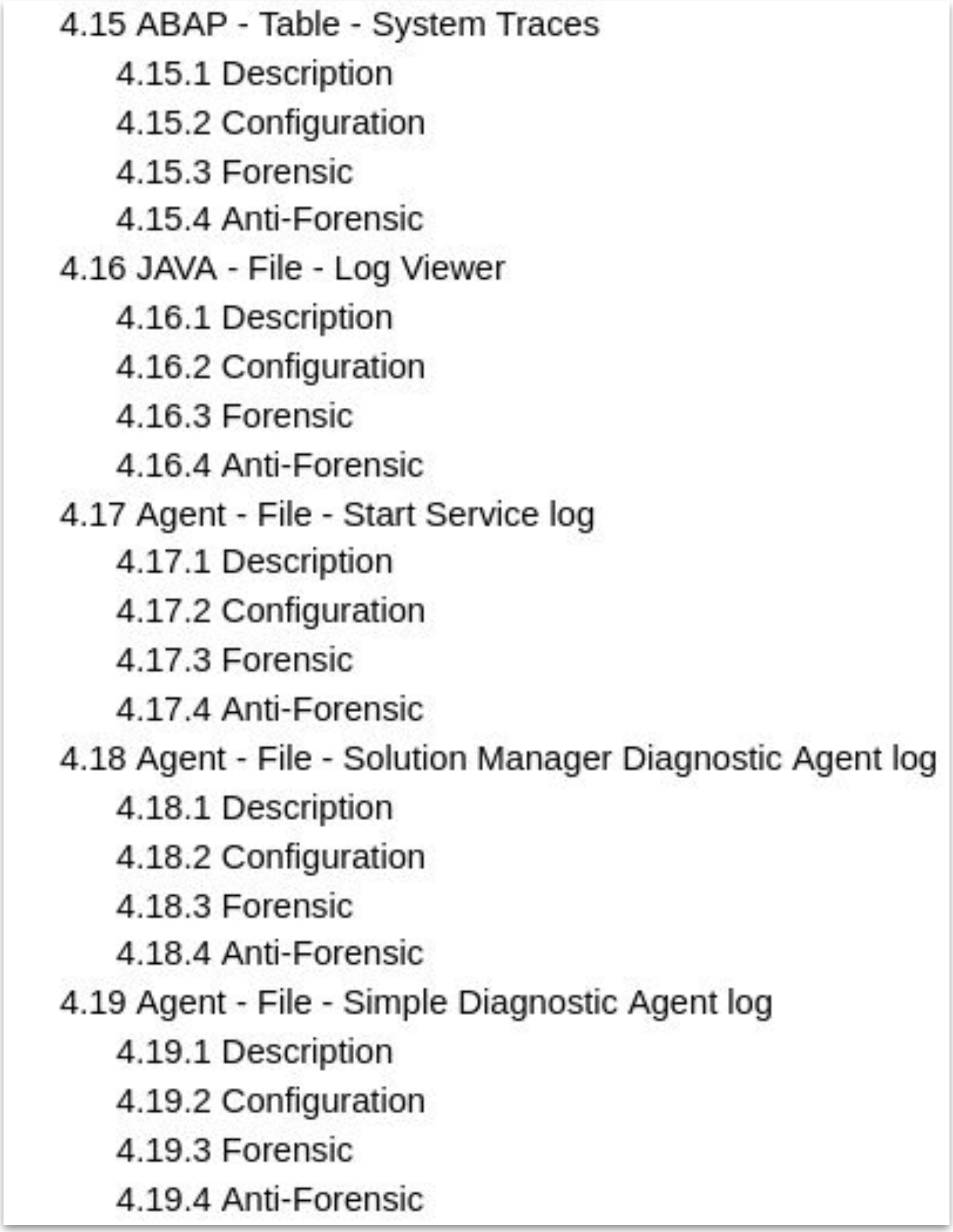
ABAP - File - Syslog	ABAP - **Table** - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - **Table** - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - **Table** - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - **Table** - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - **Table** - Change Documents	

SAP Data Sources



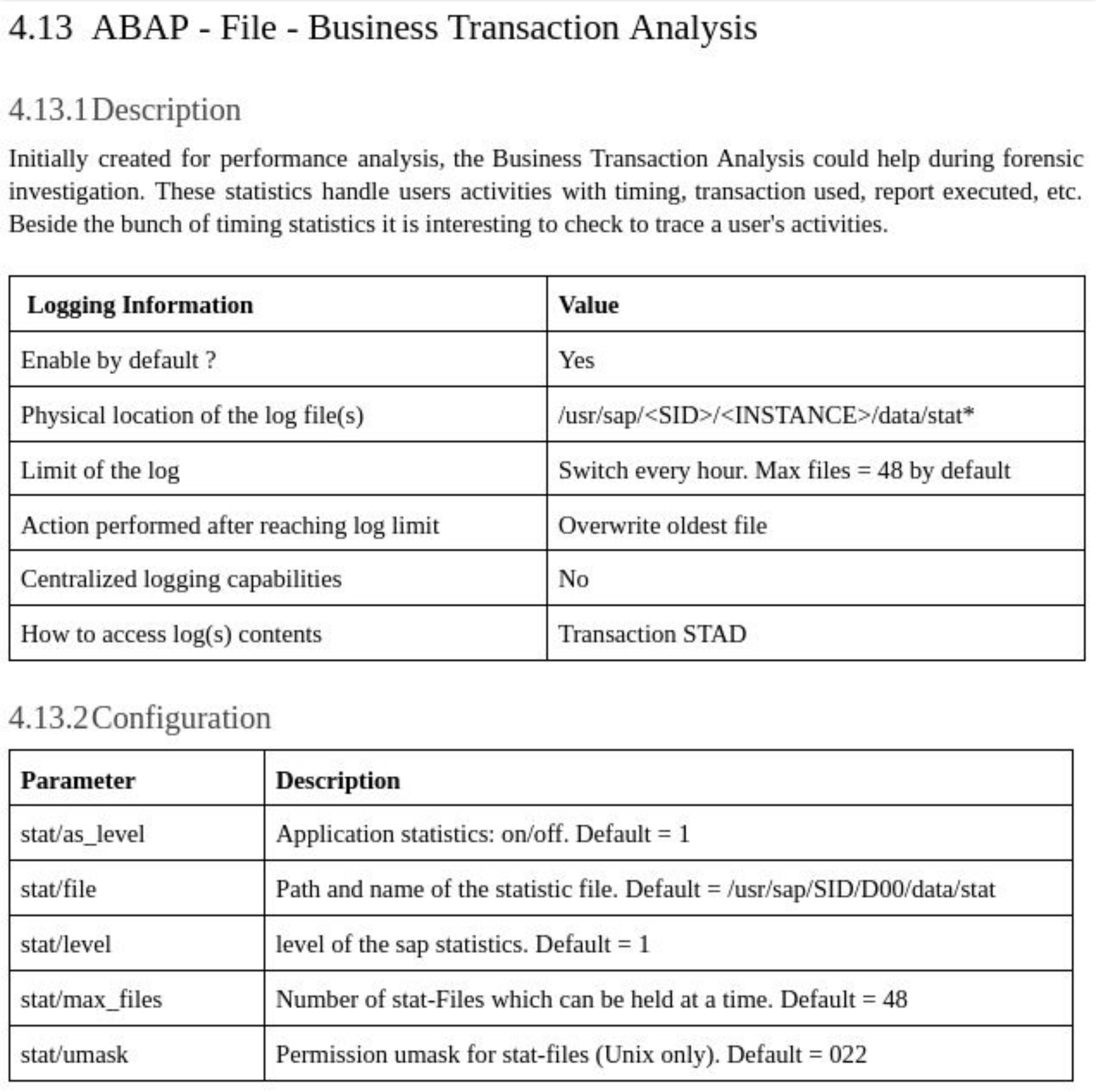
4. Data sources information

- 4.1 ABAP - File - System Trace
  - 4.1.1 Description
  - 4.1.2 Configuration
  - 4.1.3 Forensic
  - 4.1.4 Anti-Forensic
- 4.2 ABAP/JAVA - File - Developer Traces
  - 4.2.1 Description
  - 4.2.2 Configuration
  - 4.2.3 Forensic
  - 4.2.4 Anti-Forensic
- 4.3 ABAP - File - Security Audit Log (SAL)
  - 4.3.1 Description
  - 4.3.2 Configuration
  - 4.3.3 Forensic
  - 4.3.4 Anti-Forensic
- 4.4 ABAP/JAVA - File - Gateway
  - 4.4.1 Description
  - 4.4.2 Configuration
  - 4.4.3 Forensic
  - 4.4.4 Anti-Forensic
- 4.5 ABAP/JAVA - File - Message Server
  - 4.5.1 Description
  - 4.5.2 Configuration



- 4.15 ABAP - Table - System Traces
  - 4.15.1 Description
  - 4.15.2 Configuration
  - 4.15.3 Forensic
  - 4.15.4 Anti-Forensic
- 4.16 JAVA - File - Log Viewer
  - 4.16.1 Description
  - 4.16.2 Configuration
  - 4.16.3 Forensic
  - 4.16.4 Anti-Forensic
- 4.17 Agent - File - Start Service log
  - 4.17.1 Description
  - 4.17.2 Configuration
  - 4.17.3 Forensic
  - 4.17.4 Anti-Forensic
- 4.18 Agent - File - Solution Manager Diagnostic Agent log
  - 4.18.1 Description
  - 4.18.2 Configuration
  - 4.18.3 Forensic
  - 4.18.4 Anti-Forensic
- 4.19 Agent - File - Simple Diagnostic Agent log
  - 4.19.1 Description
  - 4.19.2 Configuration
  - 4.19.3 Forensic
  - 4.19.4 Anti-Forensic

SAP Data Sources



4.13 ABAP - File - Business Transaction Analysis

4.13.1 Description

Initially created for performance analysis, the Business Transaction Analysis could help during forensic investigation. These statistics handle users activities with timing, transaction used, report executed, etc. Beside the bunch of timing statistics it is interesting to check to trace a user's activities.

Logging Information	Value
Enable by default ?	Yes
Physical location of the log file(s)	/usr/sap/<SID>/<INSTANCE>/data/stat*
Limit of the log	Switch every hour. Max files = 48 by default
Action performed after reaching log limit	Overwrite oldest file
Centralized logging capabilities	No
How to access log(s) contents	Transaction STAD

4.13.2 Configuration

Parameter	Description
stat/as_level	Application statistics: on/off. Default = 1
stat/file	Path and name of the statistic file. Default = /usr/sap/SID/D00/data/stat
stat/level	level of the sap statistics. Default = 1
stat/max_files	Number of stat-Files which can be held at a time. Default = 48
stat/umask	Permission umask for stat-files (Unix only). Default = 022

AGENDA

0x01	Why SAP Forensic ?
0x02	The White Paper
0x03	SAP Data Sources
0x04	**Good to know…**
0x05	Closing part

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

SAP Data Sources

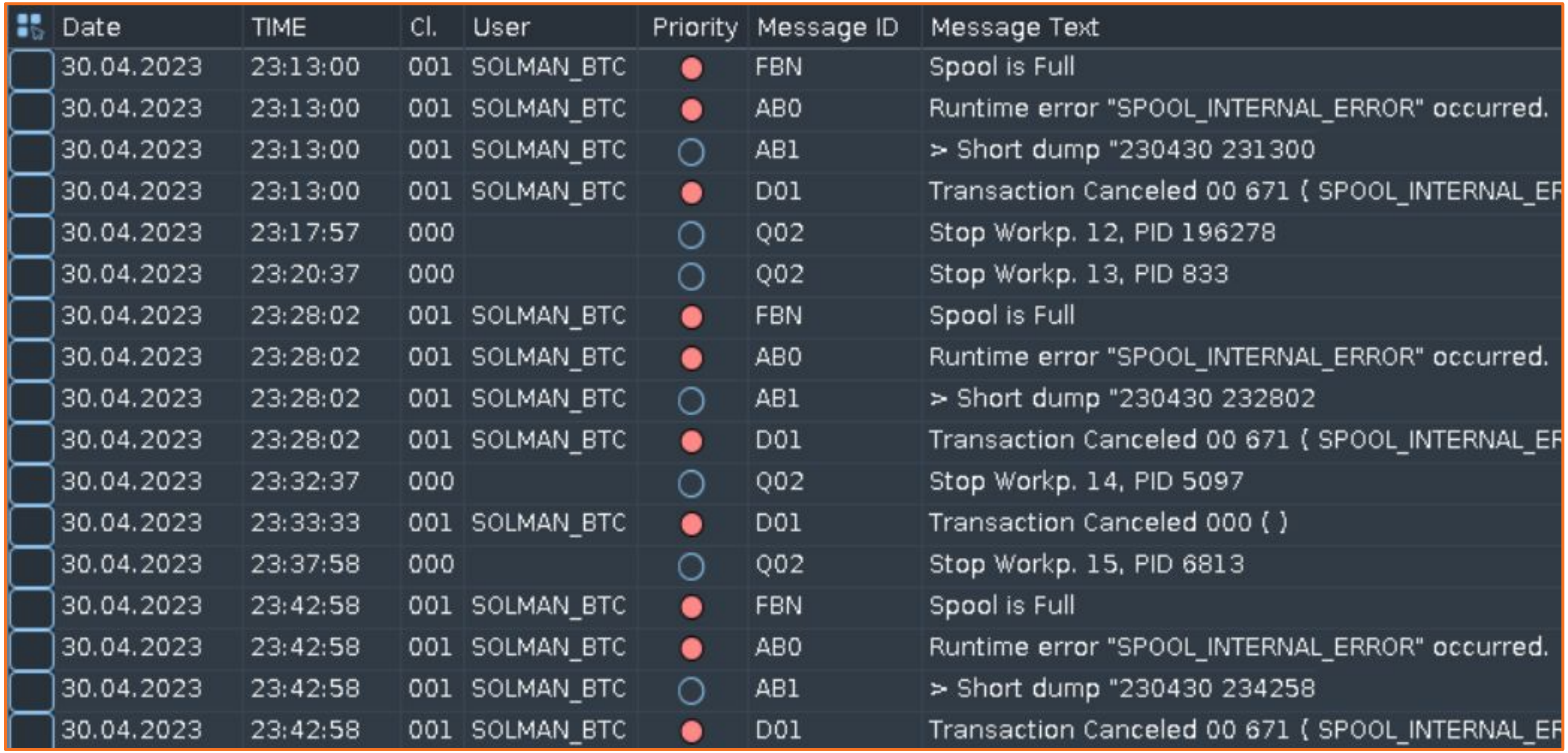
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP - File - Syslog

- Centralized log present in all SAP system ABAP
- Windows OS Event or Unix /var/log/message equivalent for SAP

ABAP - File - Syslog

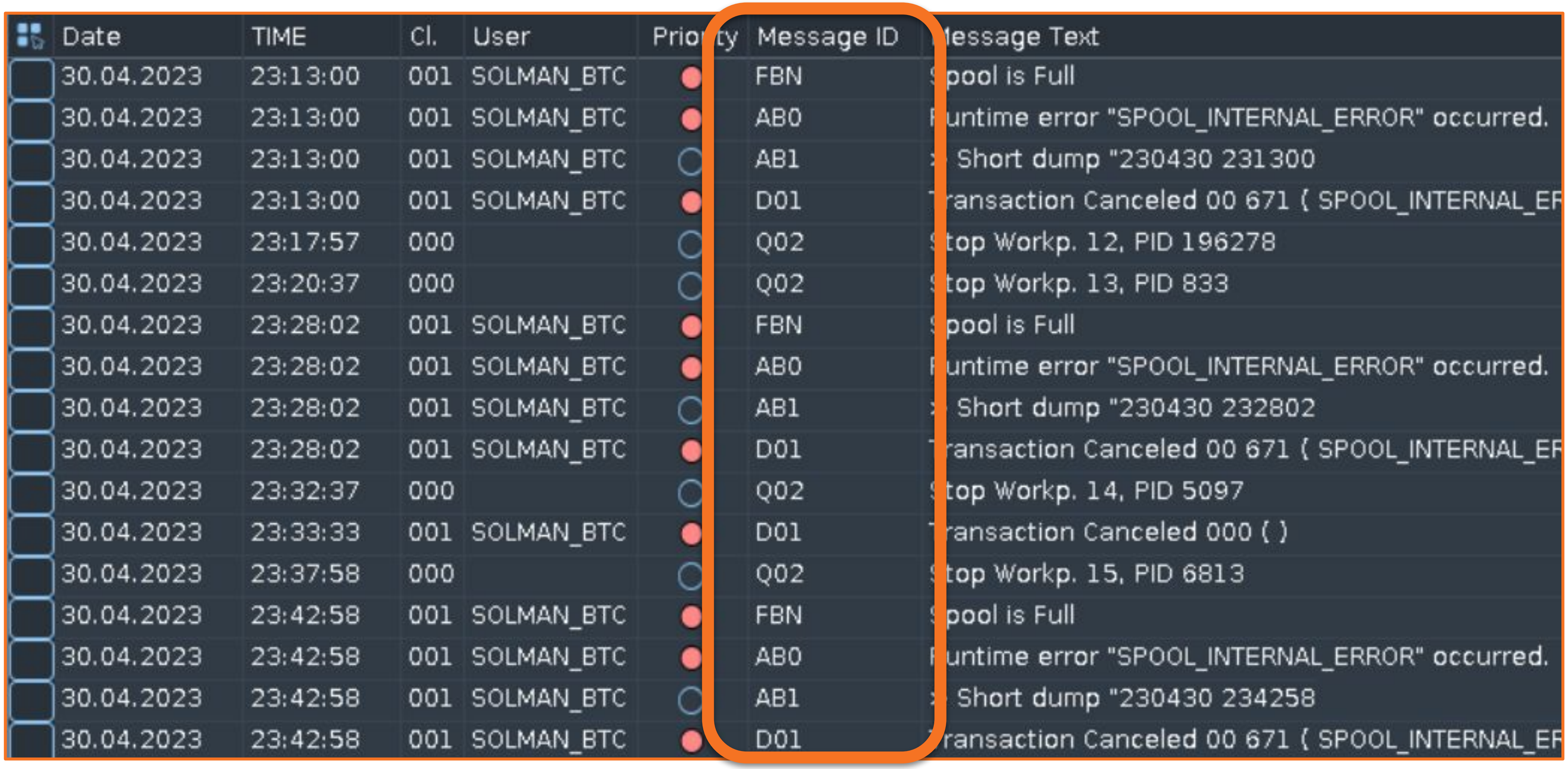
- Centralized log present in all SAP system ABAP
- Windows OS Event or Unix /var/log/message equivalent for SAP



	Date	TIME	Cl.	User	Priority	Message ID	Message Text
	30.04.2023	23:13:00	001	SOLMAN_BTC	●	FBN	Spool is Full
	30.04.2023	23:13:00	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
	30.04.2023	23:13:00	001	SOLMAN_BTC	○	AB1	> Short dump "230430 231300
	30.04.2023	23:13:00	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_EF
	30.04.2023	23:17:57	000		○	Q02	Stop Workp. 12, PID 196278
	30.04.2023	23:20:37	000		○	Q02	Stop Workp. 13, PID 833
	30.04.2023	23:28:02	001	SOLMAN_BTC	●	FBN	Spool is Full
	30.04.2023	23:28:02	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
	30.04.2023	23:28:02	001	SOLMAN_BTC	○	AB1	> Short dump "230430 232802
	30.04.2023	23:28:02	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_EF
	30.04.2023	23:32:37	000		○	Q02	Stop Workp. 14, PID 5097
	30.04.2023	23:33:33	001	SOLMAN_BTC	●	D01	Transaction Canceled 000 ( )
	30.04.2023	23:37:58	000		○	Q02	Stop Workp. 15, PID 6813
	30.04.2023	23:42:58	001	SOLMAN_BTC	●	FBN	Spool is Full
	30.04.2023	23:42:58	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
	30.04.2023	23:42:58	001	SOLMAN_BTC	○	AB1	> Short dump "230430 234258
	30.04.2023	23:42:58	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_EF

ABAP - File - Syslog

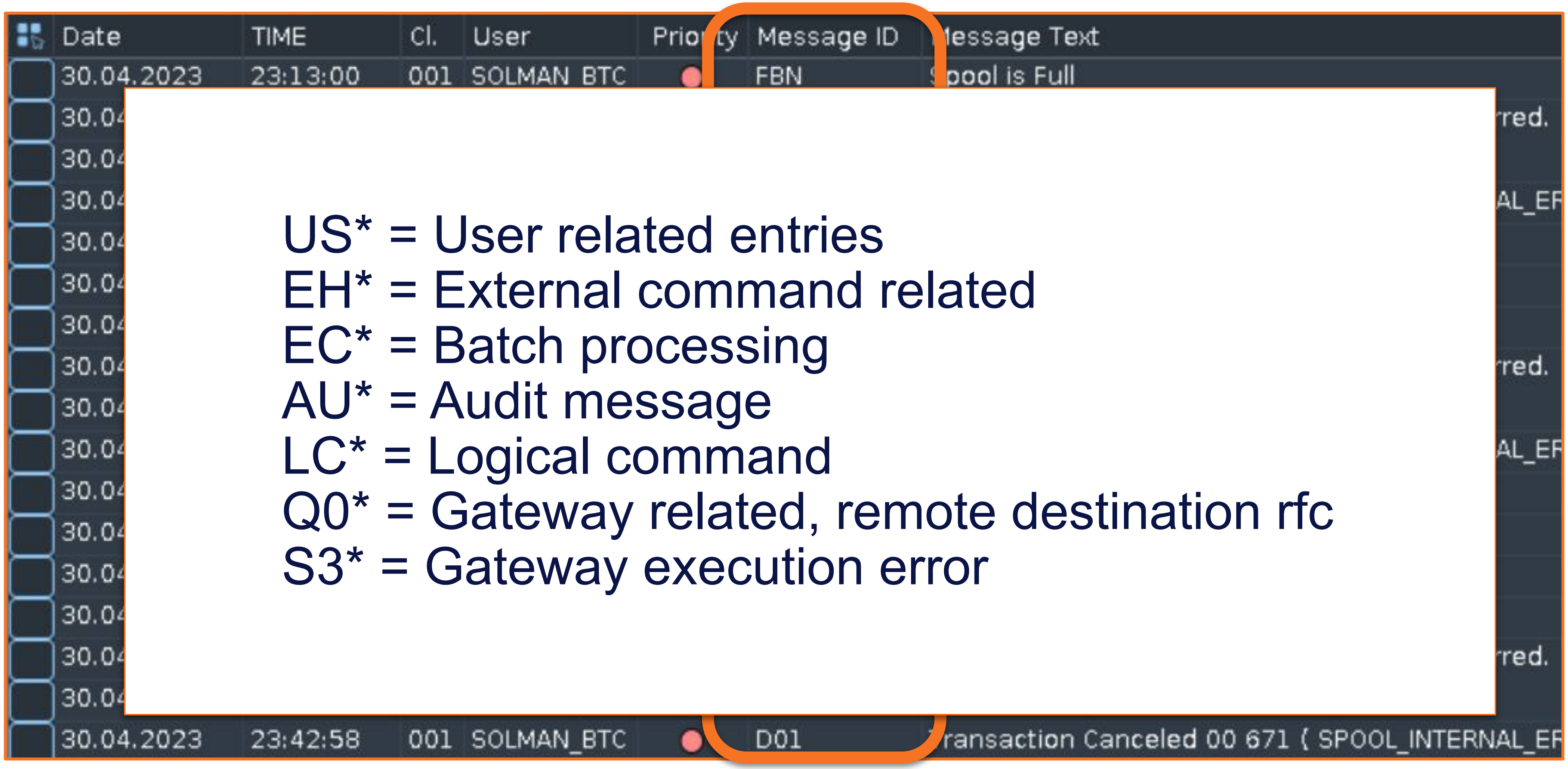
- Centralized log present in all SAP system ABAP
- Windows OS Event or Unix /var/log/message equivalent for SAP



Date	TIME	Cl.	User	Priority	Message ID	Message Text
30.04.2023	23:13:00	001	SOLMAN_BTC	●	FBN	Spool is Full
30.04.2023	23:13:00	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
30.04.2023	23:13:00	001	SOLMAN_BTC	○	AB1	> Short dump "230430 231300
30.04.2023	23:13:00	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_ER
30.04.2023	23:17:57	000		○	Q02	Stop Workp. 12, PID 196278
30.04.2023	23:20:37	000		○	Q02	Stop Workp. 13, PID 833
30.04.2023	23:28:02	001	SOLMAN_BTC	●	FBN	Spool is Full
30.04.2023	23:28:02	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
30.04.2023	23:28:02	001	SOLMAN_BTC	○	AB1	> Short dump "230430 232802
30.04.2023	23:28:02	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_ER
30.04.2023	23:32:37	000		○	Q02	Stop Workp. 14, PID 5097
30.04.2023	23:33:33	001	SOLMAN_BTC	●	D01	Transaction Canceled 000 ( )
30.04.2023	23:37:58	000		○	Q02	Stop Workp. 15, PID 6813
30.04.2023	23:42:58	001	SOLMAN_BTC	●	FBN	Spool is Full
30.04.2023	23:42:58	001	SOLMAN_BTC	●	AB0	Runtime error "SPOOL_INTERNAL_ERROR" occurred.
30.04.2023	23:42:58	001	SOLMAN_BTC	○	AB1	> Short dump "230430 234258
30.04.2023	23:42:58	001	SOLMAN_BTC	●	D01	Transaction Canceled 00 671 (SPOOL_INTERNAL_ER

ABAP - File - Syslog

- Centralized log present in all SAP system ABAP
- Windows OS Event or Unix /var/log/message equivalent for SAP



```
Date        TIME      Cl.  User         Priority  Message ID  Message Text
30.04.2023  23:13:00  001  SOLMAN_BTC   ●         FBN         Spool is Full
30.04                                                                  red.
30.04
30.04                                                                 AL_EF
30.04
30.04
30.04
30.04                                                                  red.
30.04
30.04                                                                 AL_EF
30.04
30.04
30.04
30.04
30.04                                                                  red.
30.04
30.04.2023  23:42:58  001  SOLMAN_BTC   ●         D01         Transaction Canceled 00 671 ( SPOOL_INTERNAL_EF
```

US* = User related entries
EH* = External command related
EC* = Batch processing
AU* = Audit message
LC* = Logical command
Q0* = Gateway related, remote destination rfc
S3* = Gateway execution error

ABAP - File - Syslog

rslg/local/file	Local Log File Name
rslg/max_diskspace/local	Maximum size of the local syslog file
rslg/messages/flat_file	File path where custom message can be stored (list of message template SE92)
rslg/unix_syslog/active	Enable/disable writing of SAP system log to unix syslog
rslg/unix_syslog/facility	Precise the syslog facility
rslg/write_sync_disk	Force synchronous write to disk if set to one. Allows operating system's cache to be used when set to zero

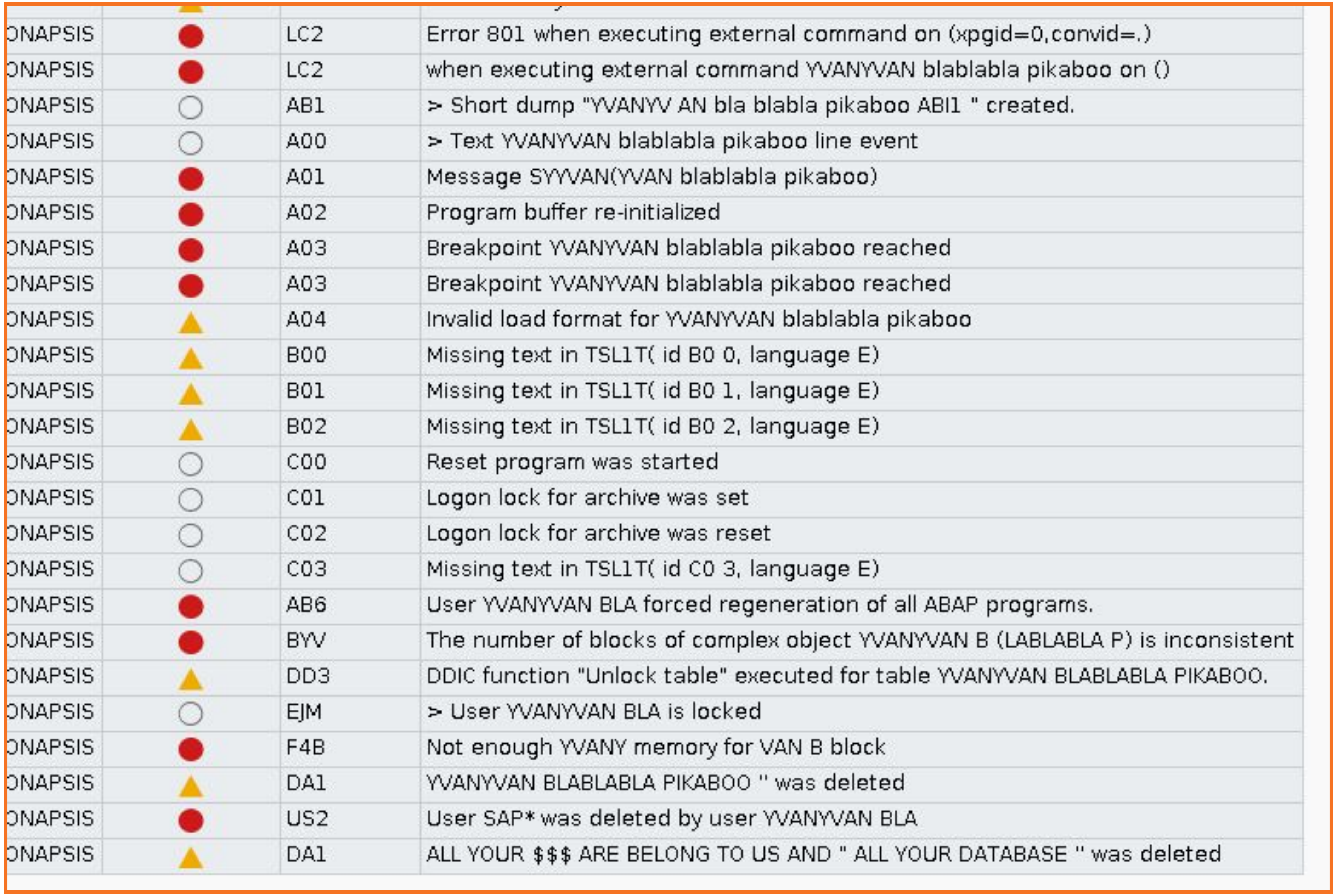
ABAP - File - Syslog

rslg/local/file	Local Log File Name
rslg/max_diskspace/local	**Maximum size of the local syslog file**
rslg/messages/flat_file	File path where custom message can be stored
rslg/unix_	
rslg/unix_	
rslg/write	

If the limit is reached, the oldest entries are overwritten

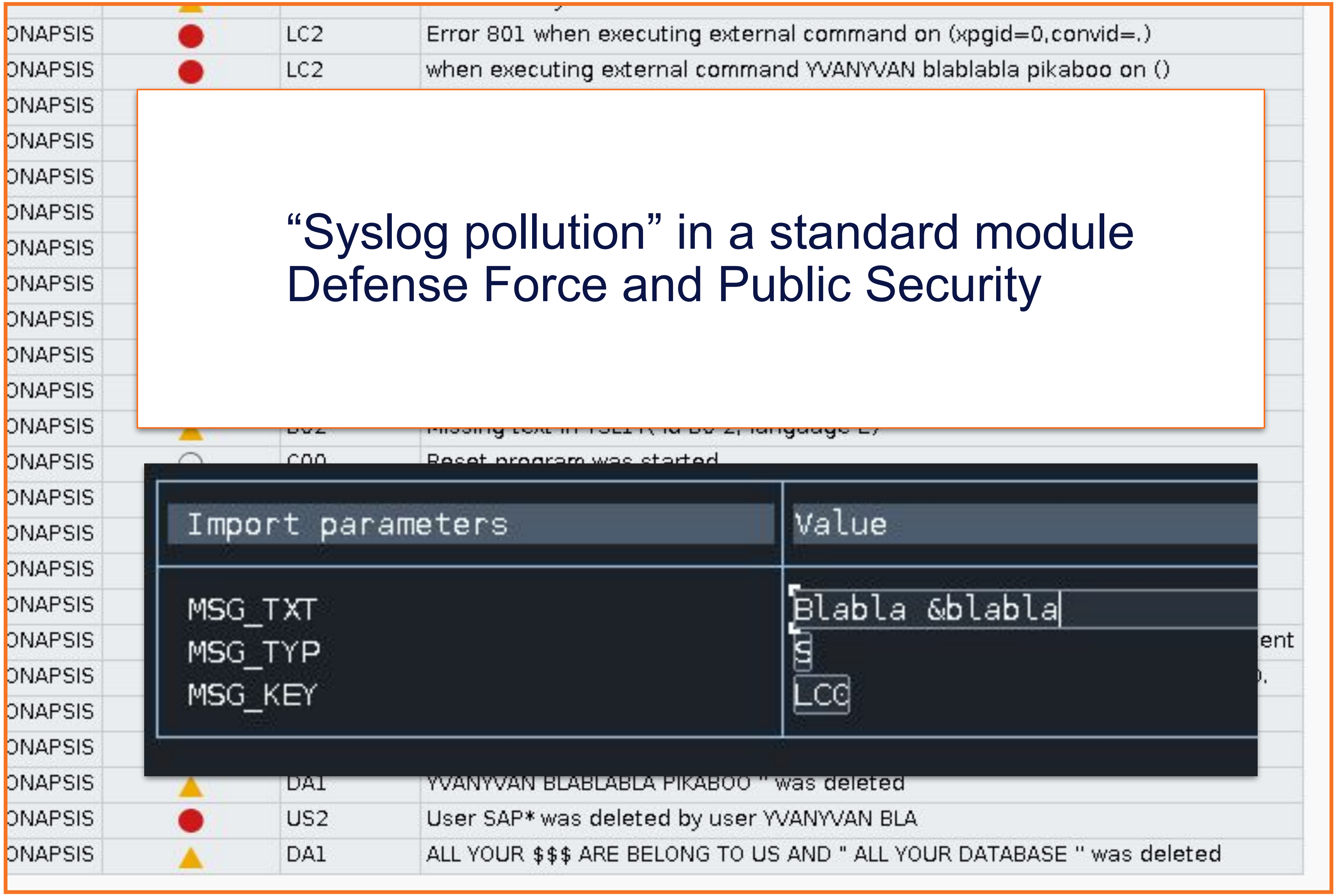
Default = 10M ~= 15000 entries
High workload system = **few hours**
Low workload system = several weeks

ABAP - File - Syslog



ONAPSIS	●	LC2	Error 801 when executing external command on (xpgid=0,convid=.)
ONAPSIS	●	LC2	when executing external command YVANYVAN blablabla pikaboo on ()
ONAPSIS	○	AB1	> Short dump "YVANYV AN bla blabla pikaboo ABI1 " created.
ONAPSIS	○	A00	> Text YVANYVAN blablabla pikaboo line event
ONAPSIS	●	A01	Message SYYVAN(YVAN blablabla pikaboo)
ONAPSIS	●	A02	Program buffer re-initialized
ONAPSIS	●	A03	Breakpoint YVANYVAN blablabla pikaboo reached
ONAPSIS	●	A03	Breakpoint YVANYVAN blablabla pikaboo reached
ONAPSIS	▲	A04	Invalid load format for YVANYVAN blablabla pikaboo
ONAPSIS	▲	B00	Missing text in TSL1T(id B0 0, language E)
ONAPSIS	▲	B01	Missing text in TSL1T(id B0 1, language E)
ONAPSIS	▲	B02	Missing text in TSL1T(id B0 2, language E)
ONAPSIS	○	C00	Reset program was started
ONAPSIS	○	C01	Logon lock for archive was set
ONAPSIS	○	C02	Logon lock for archive was reset
ONAPSIS	○	C03	Missing text in TSL1T(id C0 3, language E)
ONAPSIS	●	AB6	User YVANYVAN BLA forced regeneration of all ABAP programs.
ONAPSIS	●	BYV	The number of blocks of complex object YVANYVAN B (LABLABLA P) is inconsistent
ONAPSIS	▲	DD3	DDIC function "Unlock table" executed for table YVANYVAN BLABLABLA PIKABOO.
ONAPSIS	○	EJM	> User YVANYVAN BLA is locked
ONAPSIS	●	F4B	Not enough YVANY memory for VAN B block
ONAPSIS	▲	DA1	YVANYVAN BLABLABLA PIKABOO " was deleted
ONAPSIS	●	US2	User SAP* was deleted by user YVANYVAN BLA
ONAPSIS	▲	DA1	ALL YOUR $$$ ARE BELONG TO US AND " ALL YOUR DATABASE " was deleted

ABAP - File - Syslog

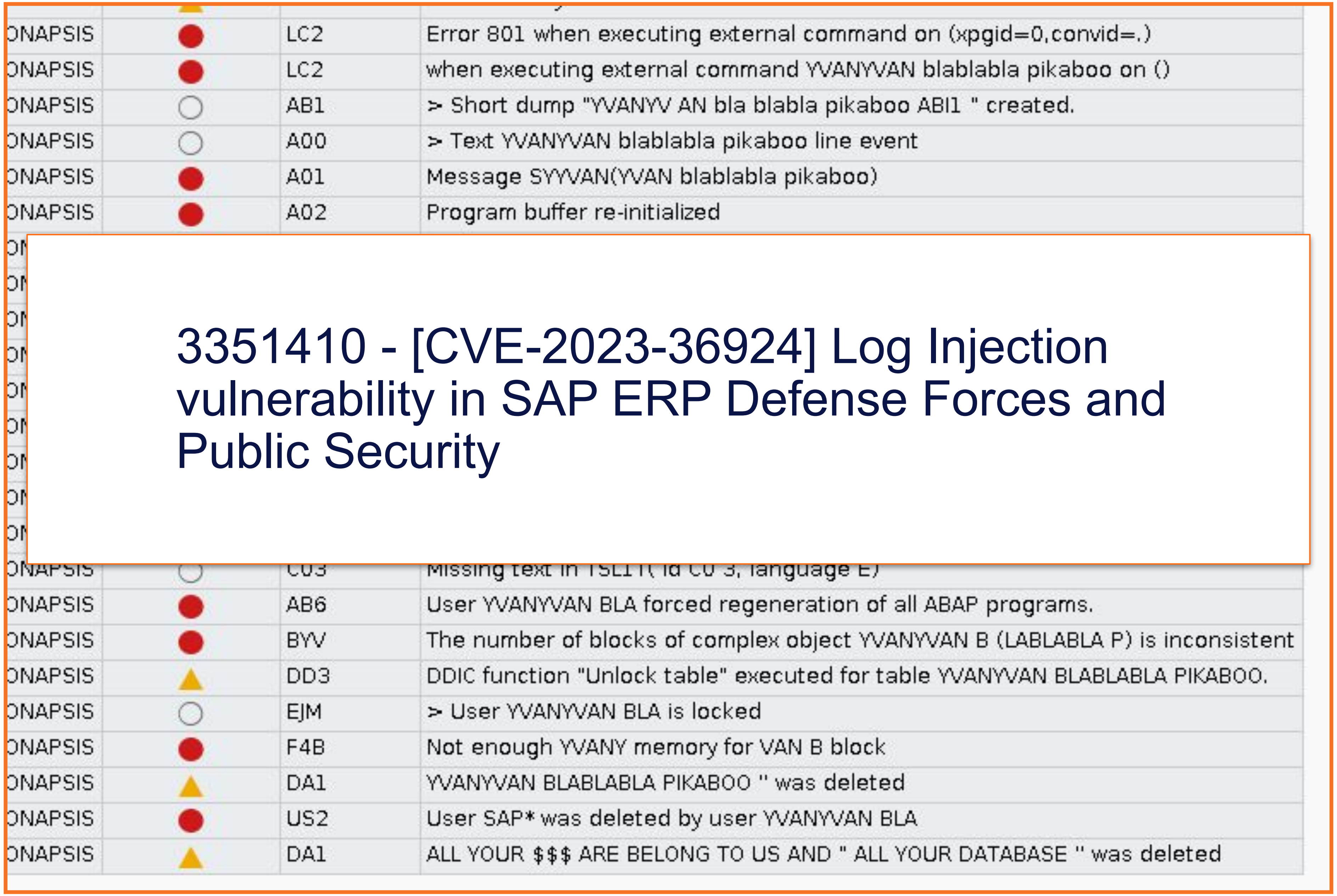


```
ONAPSIS   ●   LC2   Error 801 when executing external command on (xpgid=0,convid=.)
ONAPSIS   ●   LC2   when executing external command YVANYVAN blablabla pikaboo on ()
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS   ▲   BU2   Missing text in TSL1T( id BU 2, language E)
ONAPSIS   ○   C00   Reset program was started
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS
ONAPSIS                                                                     ent
ONAPSIS                                                                     .
ONAPSIS
ONAPSIS
ONAPSIS   ▲   DA1   YVANYVAN BLABLABLA PIKABOO '' was deleted
ONAPSIS   ●   US2   User SAP* was deleted by user YVANYVAN BLA
ONAPSIS   ▲   DA1   ALL YOUR $$$ ARE BELONG TO US AND '' ALL YOUR DATABASE '' was deleted
```

“Syslog pollution” in a standard module
Defense Force and Public Security

Import parameters	Value
MSG_TXT	Blabla &blabla
MSG_TYP	S
MSG_KEY	LCC

ABAP - File - Syslog



```
ONAPSIS  ●  LC2  Error 801 when executing external command on (xpgid=0,convid=.)
ONAPSIS  ●  LC2  when executing external command YVANYVAN blablabla pikaboo on ()
ONAPSIS  ○  AB1  > Short dump "YVANYV AN bla blabla pikaboo ABI1 " created.
ONAPSIS  ○  A00  > Text YVANYVAN blablabla pikaboo line event
ONAPSIS  ●  A01  Message SYYVAN(YVAN blablabla pikaboo)
ONAPSIS  ●  A02  Program buffer re-initialized
ONAPSIS  ○  C03  Missing text in TSL1T( id C0 3, language E)
ONAPSIS  ●  AB6  User YVANYVAN BLA forced regeneration of all ABAP programs.
ONAPSIS  ●  BYV  The number of blocks of complex object YVANYVAN B (LABLABLA P) is inconsistent
ONAPSIS  ▲  DD3  DDIC function "Unlock table" executed for table YVANYVAN BLABLABLA PIKABOO.
ONAPSIS  ○  EJM  > User YVANYVAN BLA is locked
ONAPSIS  ●  F4B  Not enough YVANY memory for VAN B block
ONAPSIS  ▲  DA1  YVANYVAN BLABLABLA PIKABOO '' was deleted
ONAPSIS  ●  US2  User SAP* was deleted by user YVANYVAN BLA
ONAPSIS  ▲  DA1  ALL YOUR $$$ ARE BELONG TO US AND " ALL YOUR DATABASE '' was deleted
```

3351410 - [CVE-2023-36924] Log Injection vulnerability in SAP ERP Defense Forces and Public Security

SAP Data Sources

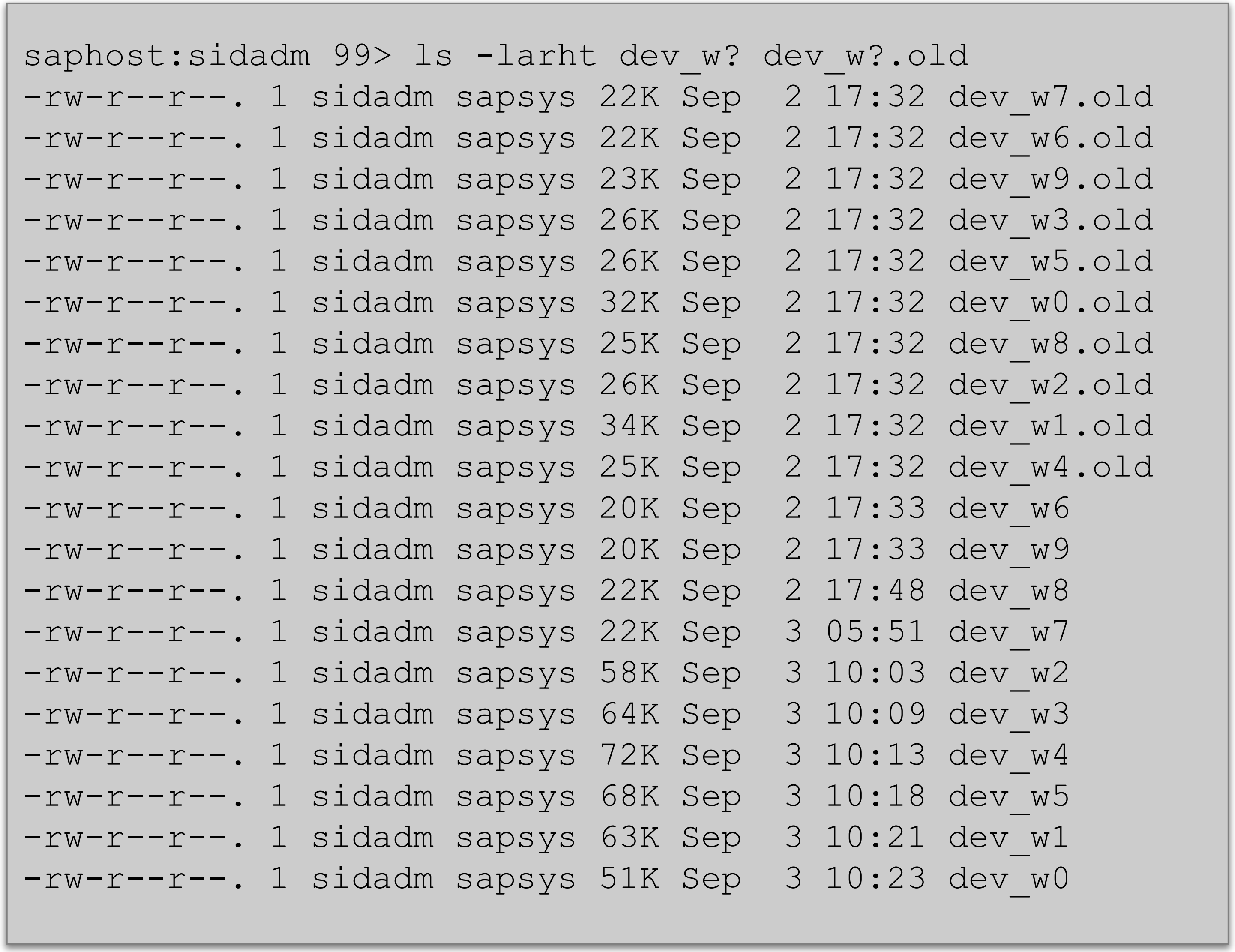
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	on Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP/JAVA - File - Developer Traces

- /usr/sap/<SID>/<INSTANCE>/work/

- During SAP System startup process, the kernel **backup the current dev files to .old** by overwriting the previous one

- If the SAP System restart more than one time after incident **they are gone**



```
saphost:sidadm 99> ls -larht dev_w? dev_w?.old
-rw-r--r--. 1 sidadm sapsys 22K Sep  2 17:32 dev_w7.old
-rw-r--r--. 1 sidadm sapsys 22K Sep  2 17:32 dev_w6.old
-rw-r--r--. 1 sidadm sapsys 23K Sep  2 17:32 dev_w9.old
-rw-r--r--. 1 sidadm sapsys 26K Sep  2 17:32 dev_w3.old
-rw-r--r--. 1 sidadm sapsys 26K Sep  2 17:32 dev_w5.old
-rw-r--r--. 1 sidadm sapsys 32K Sep  2 17:32 dev_w0.old
-rw-r--r--. 1 sidadm sapsys 25K Sep  2 17:32 dev_w8.old
-rw-r--r--. 1 sidadm sapsys 26K Sep  2 17:32 dev_w2.old
-rw-r--r--. 1 sidadm sapsys 34K Sep  2 17:32 dev_w1.old
-rw-r--r--. 1 sidadm sapsys 25K Sep  2 17:32 dev_w4.old
-rw-r--r--. 1 sidadm sapsys 20K Sep  2 17:33 dev_w6
-rw-r--r--. 1 sidadm sapsys 20K Sep  2 17:33 dev_w9
-rw-r--r--. 1 sidadm sapsys 22K Sep  2 17:48 dev_w8
-rw-r--r--. 1 sidadm sapsys 22K Sep  3 05:51 dev_w7
-rw-r--r--. 1 sidadm sapsys 58K Sep  3 10:03 dev_w2
-rw-r--r--. 1 sidadm sapsys 64K Sep  3 10:09 dev_w3
-rw-r--r--. 1 sidadm sapsys 72K Sep  3 10:13 dev_w4
-rw-r--r--. 1 sidadm sapsys 68K Sep  3 10:18 dev_w5
-rw-r--r--. 1 sidadm sapsys 63K Sep  3 10:21 dev_w1
-rw-r--r--. 1 sidadm sapsys 51K Sep  3 10:23 dev_w0
```

ABAP/JAVA - File - Developer Traces

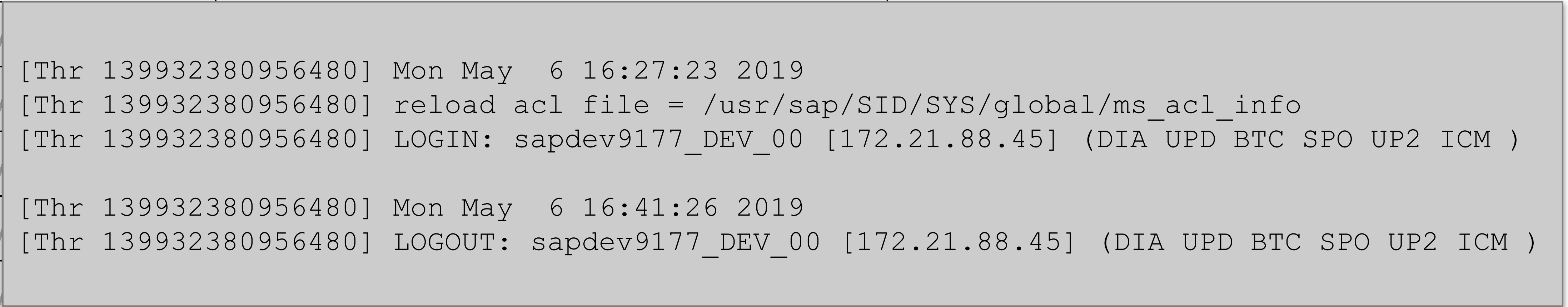
- Each service and processes have their own developer trace

File Name	SAP service or process
dev_ms	message server
dev_rd	gateway service
dev_enq	enqueue service
dev_disp	dispatcher service
dev_tp	transport process
dev_xpg	external program
dev_icm	internet communication manager
dev_icm_sec	icm security related log
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	work process

ABAP/JAVA - File - Developer Traces

- Each service and processes have their own developer trace

File Name	SAP service or process
dev_ms	**message server**
dev_rd	gateway service
dev	
dev	
dev	
dev	
dev_	
dev_icm_sec	icm security related log
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	work process



```
[Thr 139932380956480] Mon May  6 16:27:23 2019
[Thr 139932380956480] reload acl file = /usr/sap/SID/SYS/global/ms_acl_info
[Thr 139932380956480] LOGIN: sapdev9177_DEV_00 [172.21.88.45] (DIA UPD BTC SPO UP2 ICM )

[Thr 139932380956480] Mon May  6 16:41:26 2019
[Thr 139932380956480] LOGOUT: sapdev9177_DEV_00 [172.21.88.45] (DIA UPD BTC SPO UP2 ICM )
```

“Be trusted attack” or “10KBlaze” pattern

ABAP/JAVA - File - Developer Traces

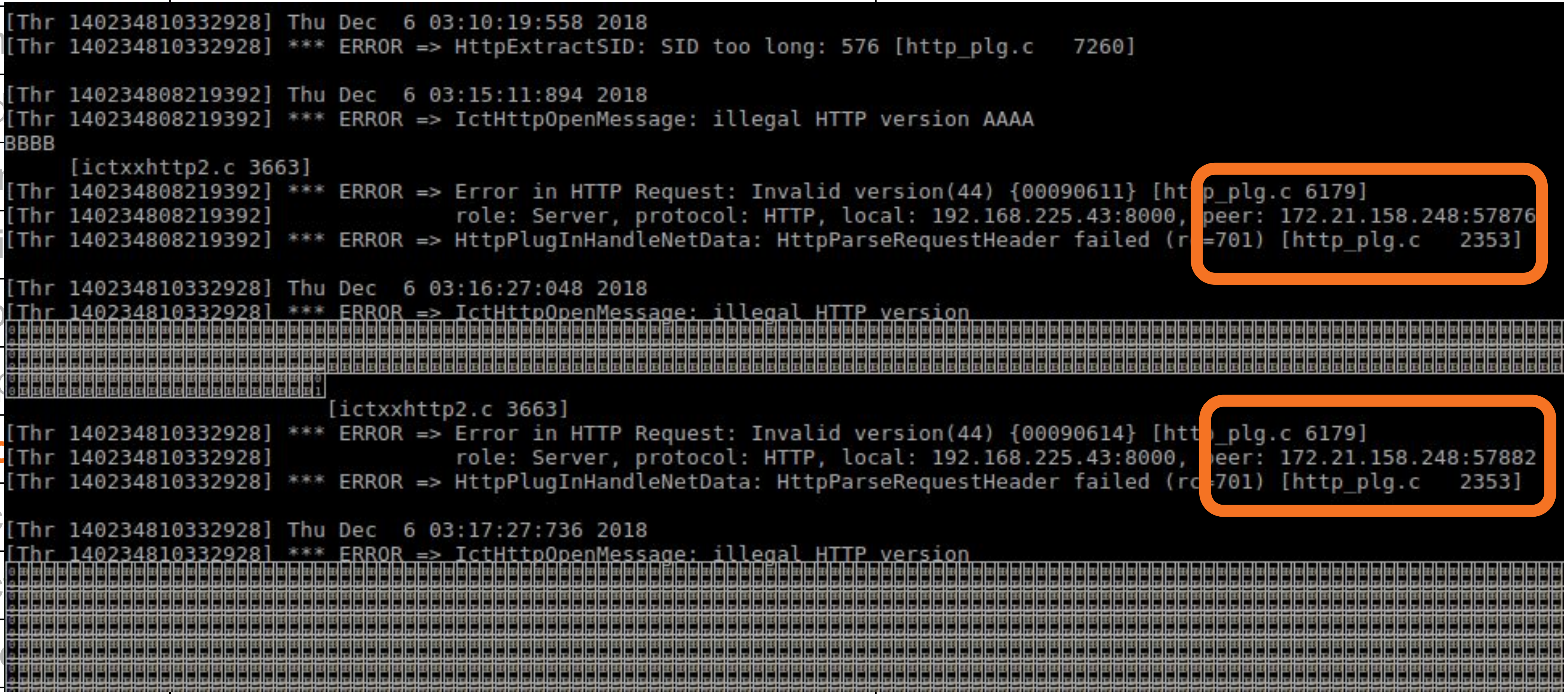
- Each service and processes have their own developer trace

File Name	SAP service or process
dev_ms	message server
dev_rd	gateway service
dev_enq	enqueue service
dev_disp	dispatcher service
dev_tp	transport process
dev_xpg	external program
dev_icm	**internet communication manager**
dev_icm_sec	icm security related log
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	work process

ABAP/JAVA - File - Developer Traces

- Each service and processes have their own developer trace

File Name	SAP service or process
dev_m	
dev_rc	
dev_er	
dev_di	
dev_tp	
dev_xp	
dev_ic	
dev_ic	
dev_ic	
dev_rf	
dev_w*	work process



```
[Thr 140234810332928] Thu Dec  6 03:10:19:558 2018
[Thr 140234810332928] *** ERROR => HttpExtractSID: SID too long: 576 [http_plg.c   7260]

[Thr 140234808219392] Thu Dec  6 03:15:11:894 2018
[Thr 140234808219392] *** ERROR => IctHttpOpenMessage: illegal HTTP version AAAA
BBBB
     [ictxxhttp2.c 3663]
[Thr 140234808219392] *** ERROR => Error in HTTP Request: Invalid version(44) {00090611} [http_plg.c 6179]
[Thr 140234808219392]                role: Server, protocol: HTTP, local: 192.168.225.43:8000, peer: 172.21.158.248:57876
[Thr 140234808219392] *** ERROR => HttpPlugInHandleNetData: HttpParseRequestHeader failed (rc=701) [http_plg.c   2353]

[Thr 140234810332928] Thu Dec  6 03:16:27:048 2018
[Thr 140234810332928] *** ERROR => IctHttpOpenMessage: illegal HTTP version

                         [ictxxhttp2.c 3663]
[Thr 140234810332928] *** ERROR => Error in HTTP Request: Invalid version(44) {00090614} [http_plg.c 6179]
[Thr 140234810332928]                role: Server, protocol: HTTP, local: 192.168.225.43:8000, peer: 172.21.158.248:57882
[Thr 140234810332928] *** ERROR => HttpPlugInHandleNetData: HttpParseRequestHeader failed (rc=701) [http_plg.c   2353]

[Thr 140234810332928] Thu Dec  6 03:17:27:736 2018
[Thr 140234810332928] *** ERROR => IctHttpOpenMessage: illegal HTTP version
```

ABAP/JAVA - File - Developer Traces

- Each service and processes have their own developer trace

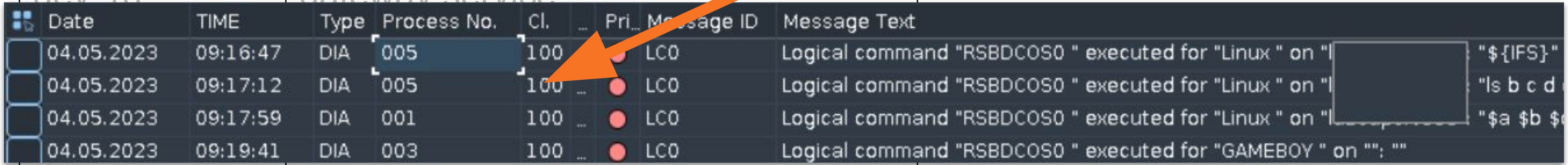
File Name	**SAP service or process**
dev_ms	message server
dev_rd	gateway service
dev_enq	enqueue service
dev_disp	dispatcher service
dev_tp	transport process
dev_xpg	external program
dev_icm	internet communication manager
dev_icm_sec	icm security related log
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	**work process**

ABAP/JAVA - File - Developer Traces

- Each service and processes have their own developer trace

File Name	SAP service or process
dev_ms	message server
dev_rd	gateway service
dev_tp	transport process
dev_xpg	external program
dev_icm	internet communication manager
dev_icm_sec	icm security related log
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	**work process**

SAP Syslog

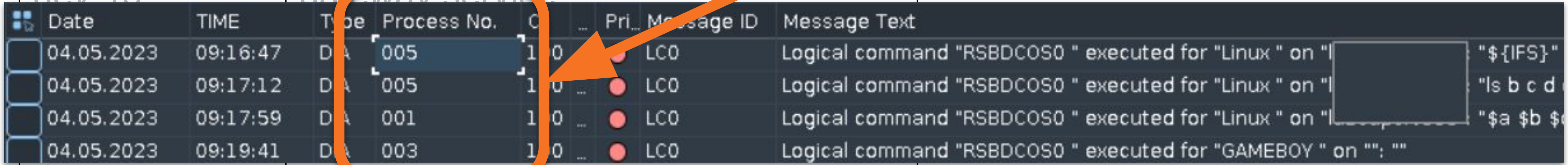


Date	TIME	Type	Process No.	Cl.	...	Pri.	Message ID	Message Text
04.05.2023	09:16:47	DIA	005	100		●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "l[redacted] "${IFS}"
04.05.2023	09:17:12	DIA	005	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "l "ls b c d
04.05.2023	09:17:59	DIA	001	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "l "$a $b $
04.05.2023	09:19:41	DIA	003	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "GAMEBOY " on "": ""

ABAP/JAVA - File - Developer Traces

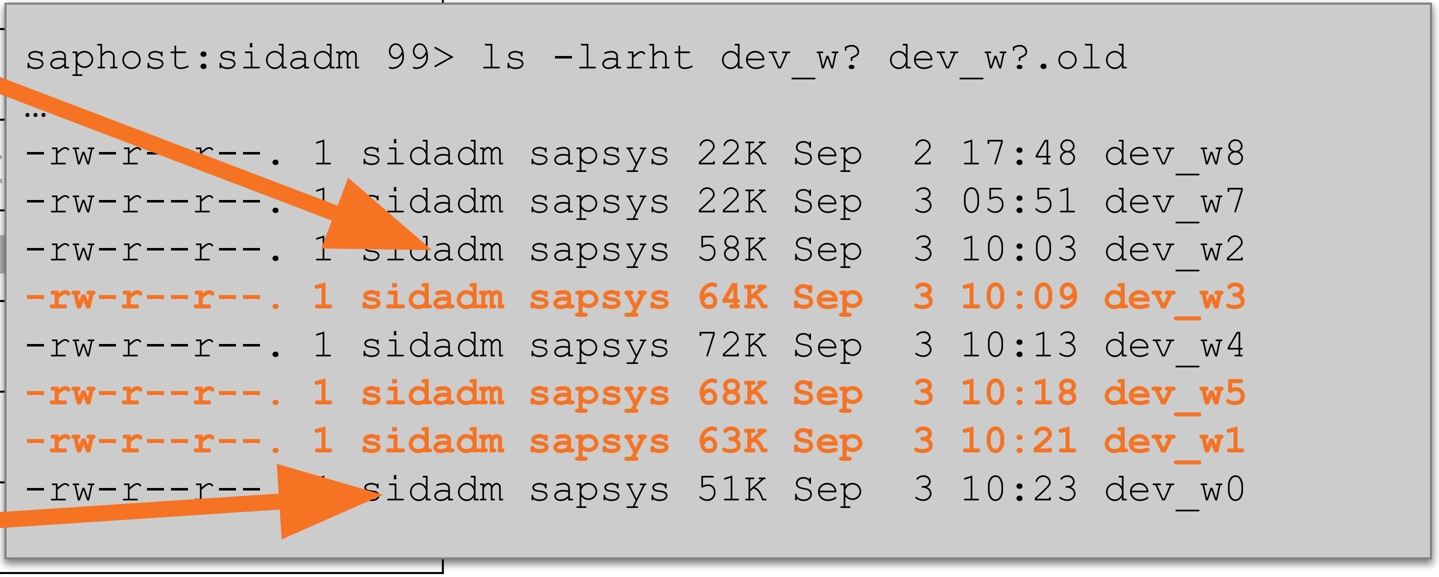
- Each service and processes have their own developer trace

File Name	SAP service or process
dev_ms	message server
dev_rd	gateway service
dev_tp	transport process
dev_xpg	external program
dev_icm	internet communicat
dev_icm_sec	icm security related l
dev_icf*	icm error log
dev_rfc*	rfc call
dev_w*	**work process**



Date	TIME	Type	Process No.	C	...	Pri...	Message ID	Message Text
04.05.2023	09:16:47	DIA	005	100		●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "[redacted] "${IFS}"
04.05.2023	09:17:12	DIA	005	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "[redacted] "ls b c d
04.05.2023	09:17:59	DIA	001	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "Linux " on "[redacted] "$a $b $
04.05.2023	09:19:41	DIA	003	100	...	●	LC0	Logical command "RSBDCOS0 " executed for "GAMEBOY " on "": ""

SAP Syslog



```
saphost:sidadm 99> ls -larht dev_w? dev_w?.old
…
-rw-r--r--. 1 sidadm sapsys 22K Sep  2 17:48 dev_w8
-rw-r--r--. 1 sidadm sapsys 22K Sep  3 05:51 dev_w7
-rw-r--r--. 1 sidadm sapsys 58K Sep  3 10:03 dev_w2
-rw-r--r--. 1 sidadm sapsys 64K Sep  3 10:09 dev_w3
-rw-r--r--. 1 sidadm sapsys 72K Sep  3 10:13 dev_w4
-rw-r--r--. 1 sidadm sapsys 68K Sep  3 10:18 dev_w5
-rw-r--r--. 1 sidadm sapsys 63K Sep  3 10:21 dev_w1
-rw-r--r--. 1 sidadm sapsys 51K Sep  3 10:23 dev_w0
```

ABAP/JAVA - File - Developer Traces

```
# decrease the trace level
saphost:sidadm $ kill -USR1 <pid_of_sap_service>

# increase the trace level
saphost:sidadm $ kill -USR2 <pid_of_sap_service>
```

ABAP/JAVA - File - Developer Traces

```
saphost:sidadm $ kill -USR1 `pidof icman`
saphost:sidadm $ kill -USR1 `pidof icman`
saphost:sidadm $ kill -USR1 `pidof icman`
```

```
[Thr 140692812900096] **** SigHandler: signal 10 received
[Thr 140692812900096] IcmSetTrcLevel: Switch trace level to: 2
[Thr 140692812900096] *
[Thr 140692812900096] * SWITCH TRC-LEVEL to 2
[Thr 140692812900096] *
[Thr 140692812900096] eppSetTraceLevel: changing trace level to 2
[Thr 140692812900096] **** SigHandlerWaiting for signal
[Thr 140692812900096] **** SigHandler: signal 10 received
[Thr 140692812900096] IcmSetTrcLevel: Switch trace level to: 1
[Thr 140692812900096] *
[Thr 140692812900096] * SWITCH TRC-LEVEL to 1
[Thr 140692812900096] *
[Thr 140692812900096] eppSetTraceLevel: changing trace level to 1
[Thr 140692812900096] **** SigHandler: signal 10 received
[Thr 140692812900096] IcmSetTrcLevel: Switch trace level to: 0
[Thr 140692812900096] *
[Thr 140692812900096] * SWITCH TRC-LEVEL to 0
[Thr 140692812900096] *
```

ABAP - File - Syslog

rdisp/TRACE_HIDE_SEC_DATA	default “on”. Display password if “off”.
rdisp/TRACE_RESOLUTION	Maximum number of time stamps in trace file per second. **0 = no timestamp written**

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	usiness Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP - File - Security Audit Log

- Not enable by default for SAP version prior 2020
- Configuration not trivial

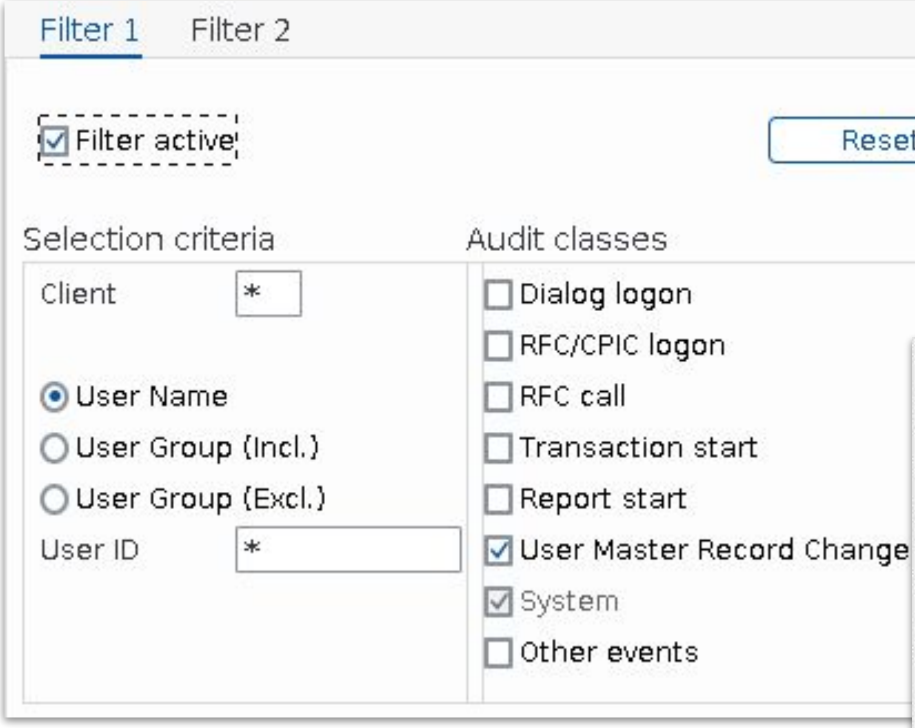
ABAP - File - Security Audit Log

- Not enable by default for SAP version prior 2020
- Configuration not trivial

rsau/enable	Enables the security audit log
rsau/local/file	Name and location of log files
rsau/integrity	Integrity Protection Format for Security Audit Log (default = 0)
rsau/log_peer_address	Recording of peer address instead of the terminal address
rsau/selection_slots	Number of filters allowed
rsau/max_diskspace/local	Maximum space for audit files
rsau/max_diskspace/per_file	Maximum size of one single security audit file
rsau/max_diskspace/per_day	Maximum size of all security audit files per day
rsau/user_selection	Defines the user selection method used inside kernel functions
DIR_AUDIT	Directory for security audit files
FN_AUDIT	Name of security audit file

ABAP - File - Security Audit Log

- Not enable by default for SAP version prior 2020
- Configuration not trivial



Filter 1 Filter 2

☑ Filter active

Reset

Selection criteria

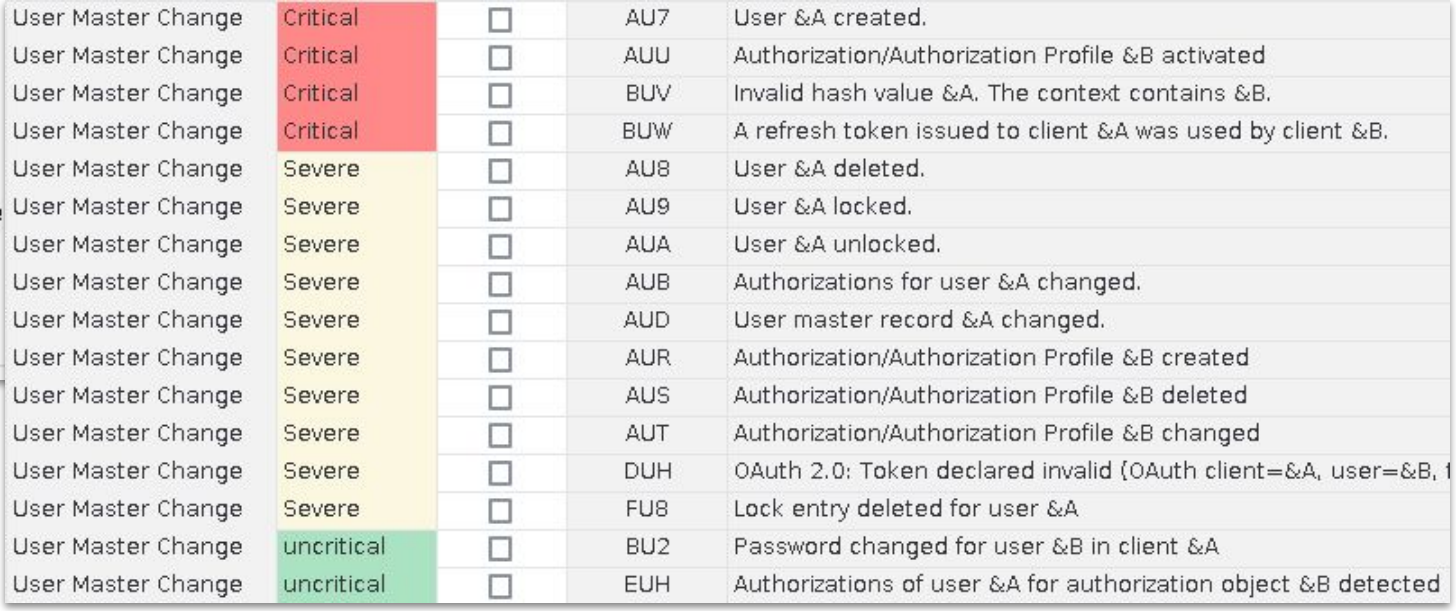
Client *

● User Name
○ User Group (Incl.)
○ User Group (Excl.)

User ID *

Audit classes

☐ Dialog logon
☐ RFC/CPIC logon
☐ RFC call
☐ Transaction start
☐ Report start
☑ User Master Record Change
☑ System
☐ Other events



User Master Change	Critical	☐	AU7	User &A created.
User Master Change	Critical	☐	AUU	Authorization/Authorization Profile &B activated
User Master Change	Critical	☐	BUV	Invalid hash value &A. The context contains &B.
User Master Change	Critical	☐	BUW	A refresh token issued to client &A was used by client &B.
User Master Change	Severe	☐	AU8	User &A deleted.
User Master Change	Severe	☐	AU9	User &A locked.
User Master Change	Severe	☐	AUA	User &A unlocked.
User Master Change	Severe	☐	AUB	Authorizations for user &A changed.
User Master Change	Severe	☐	AUD	User master record &A changed.
User Master Change	Severe	☐	AUR	Authorization/Authorization Profile &B created
User Master Change	Severe	☐	AUS	Authorization/Authorization Profile &B deleted
User Master Change	Severe	☐	AUT	Authorization/Authorization Profile &B changed
User Master Change	Severe	☐	DUH	OAuth 2.0: Token declared invalid (OAuth client=&A, user=&B,
User Master Change	Severe	☐	FU8	Lock entry deleted for user &A
User Master Change	uncritical	☐	BU2	Password changed for user &B in client &A
User Master Change	uncritical	☐	EUH	Authorizations of user &A for authorization object &B detected

ABAP - File - Security Audit Log

- Not enable by default for SAP version prior 2020
- Configuration not trivial

Bad configuration = useless :(

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	wer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP/JAVA - File - ICM Service

- Internet Communication Service

ABAP/JAVA - File - ICM Service

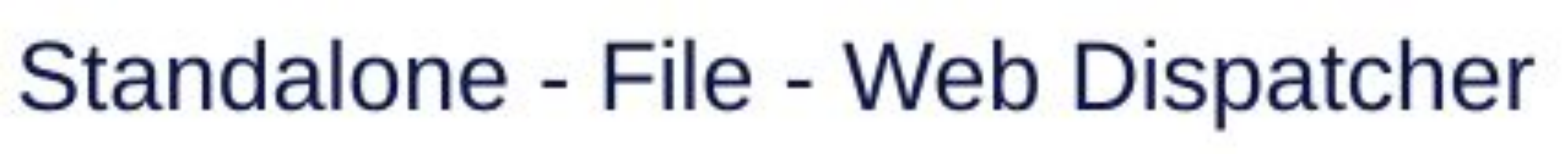
- Internet Communication Service
    - Standard user bruteforce
    - Dangerous web services were accessed
    - Number of different mandant access
    - List all unique hostname and ip involved

ABAP/JAVA - File - ICM Service

- Internet Communication Service
    - Standard user brutef
    - Dangerous web serv
    - Number of different r
    - List all unique hostna

/sap/bc/FormToRfc
/sap/bc/soap/rfc
/sap/bc/gui/sap/its/webgui
/sap/public/info
/sap/public/icf_info/logon_groups
/sap/public/bsp/sap/public
/sap/public/icf_info/urlprefix
/ctc/servlet/com.sap.ctc.util.ConfigServlet
/CTCWebService/CTCWebServiceBean
/EemAdminService
…

SAP Data Sources

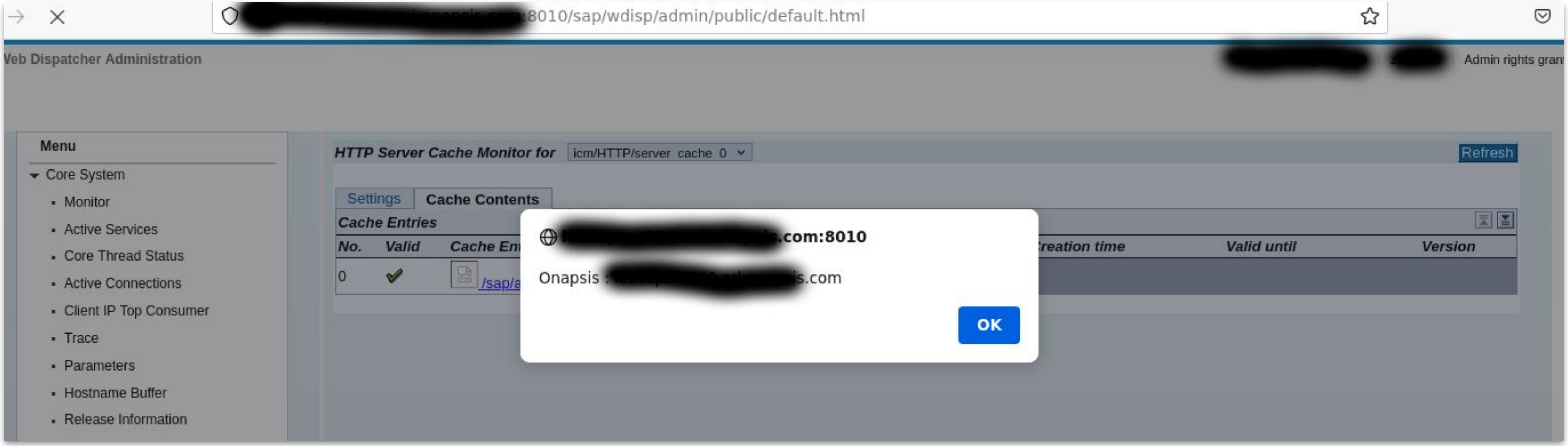
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
 Standalone - File - Web Dispatcher	rvice log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

Standalone - File - Web Dispatcher

- Reverse proxy and load balancer for incoming HTTP(S) requests

Standalone - File - Web Dispatcher

- Reverse proxy and load balancer for incoming HTTP(S) requests



[redacted]:8010/sap/wdisp/admin/public/default.html

Veb Dispatcher Administration

[redacted] [redacted] Admin rights grant

Menu

- Core System
  - Monitor
  - Active Services
  - Core Thread Status
  - Active Connections
  - Client IP Top Consumer
  - Trace
  - Parameters
  - Hostname Buffer
  - Release Information

HTTP Server Cache Monitor for icm/HTTP/server_cache_0 Refresh

Settings | Cache Contents

Cache Entries

No.	Valid	Cache En	reation time	Valid until	Version
0	✓	/sap/a			

[redacted].com:8010

Onapsis : [redacted]s.com

OK

https://launchpad.support.sap.com/#/notes/3145046

SAP Data Sources

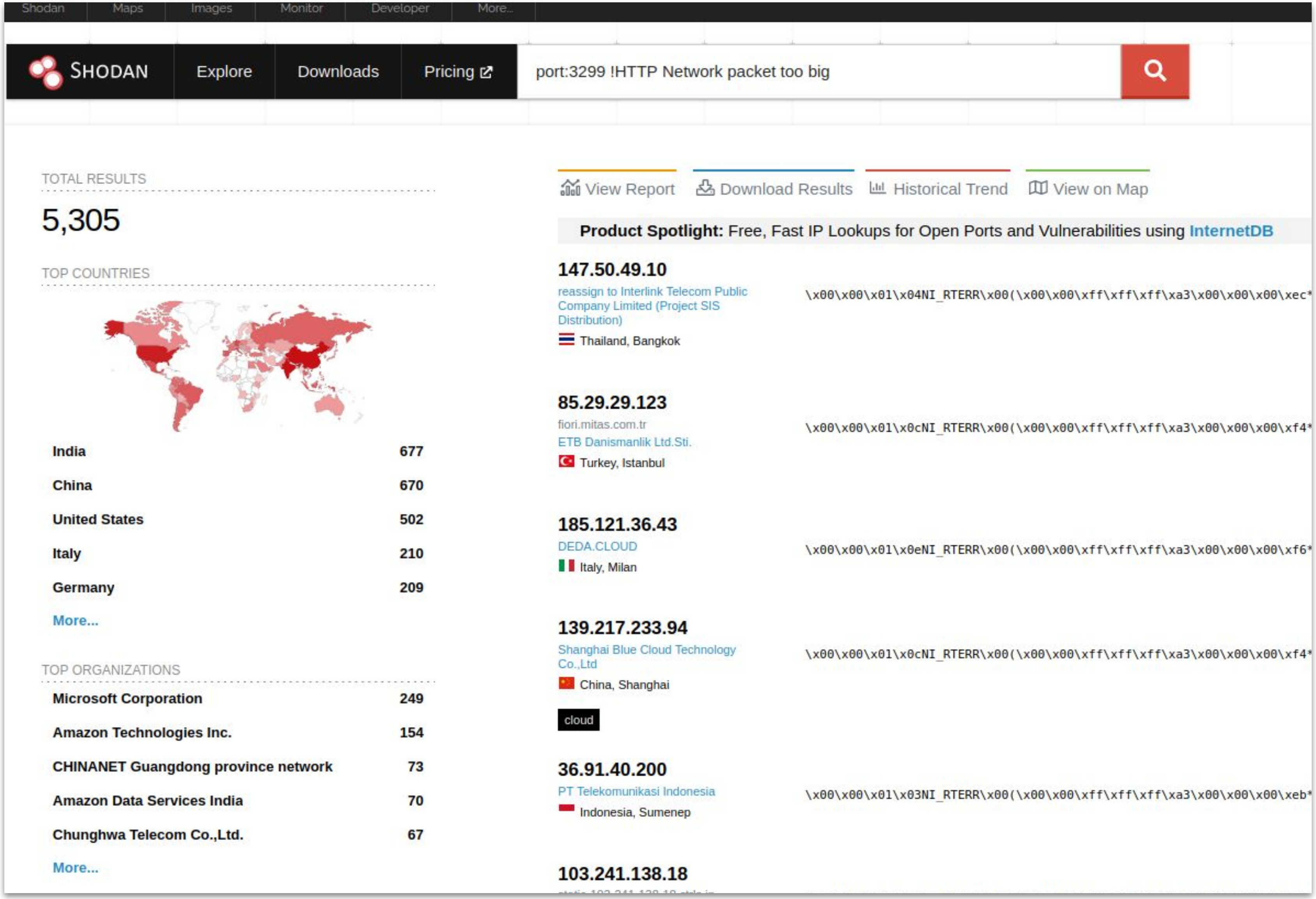
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	ution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

Standalone - File - SAPRouter Log

- Reverse proxy for SAP Protocol

Standalone - File - SAPRouter Log

- Reverse proxy for SAP Protocol



```
port:3299 !HTTP Network packet too big
```

TOTAL RESULTS

5,305

TOP COUNTRIES

India	677
China	670
United States	502
Italy	210
Germany	209

More...

TOP ORGANIZATIONS

Microsoft Corporation	249
Amazon Technologies Inc.	154
CHINANET Guangdong province network	73
Amazon Data Services India	70
Chunghwa Telecom Co.,Ltd.	67

More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

147.50.49.10
reassign to Interlink Telecom Public Company Limited (Project SIS Distribution)
Thailand, Bangkok

```
\x00\x00\x01\x04NI_RTERR\x00(\x00\x00\xff\xff\xff\xa3\x00\x00\x00\xec*
```

85.29.29.123
fiori.mitas.com.tr
ETB Danismanlik Ltd.Sti.
Turkey, Istanbul

```
\x00\x00\x01\x0cNI_RTERR\x00(\x00\x00\xff\xff\xff\xa3\x00\x00\x00\xf4*
```

185.121.36.43
DEDA.CLOUD
Italy, Milan

```
\x00\x00\x01\x0eNI_RTERR\x00(\x00\x00\xff\xff\xff\xa3\x00\x00\x00\xf6*
```

139.217.233.94
Shanghai Blue Cloud Technology Co.,Ltd
China, Shanghai
cloud

```
\x00\x00\x01\x0cNI_RTERR\x00(\x00\x00\xff\xff\xff\xa3\x00\x00\x00\xf4*
```

36.91.40.200
PT Telekomunikasi Indonesia
Indonesia, Sumenep

```
\x00\x00\x01\x03NI_RTERR\x00(\x00\x00\xff\xff\xff\xa3\x00\x00\x00\xeb*
```

103.241.138.18

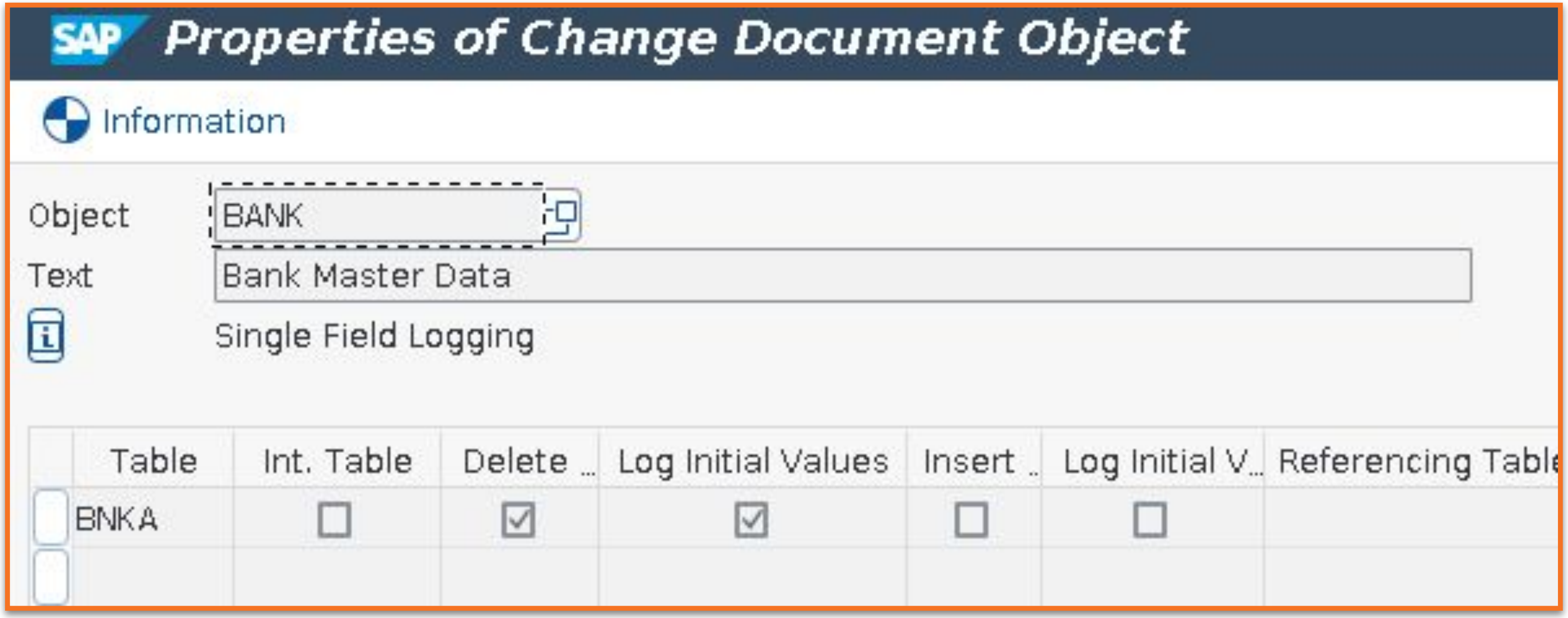
SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP - Table - Change Documents

- Standard feature
- Log change of critical objects (delete, insert, update)
- Object is a group of tables or reports

ABAP - Table - Change Documents



Properties of Change Document Object

Information

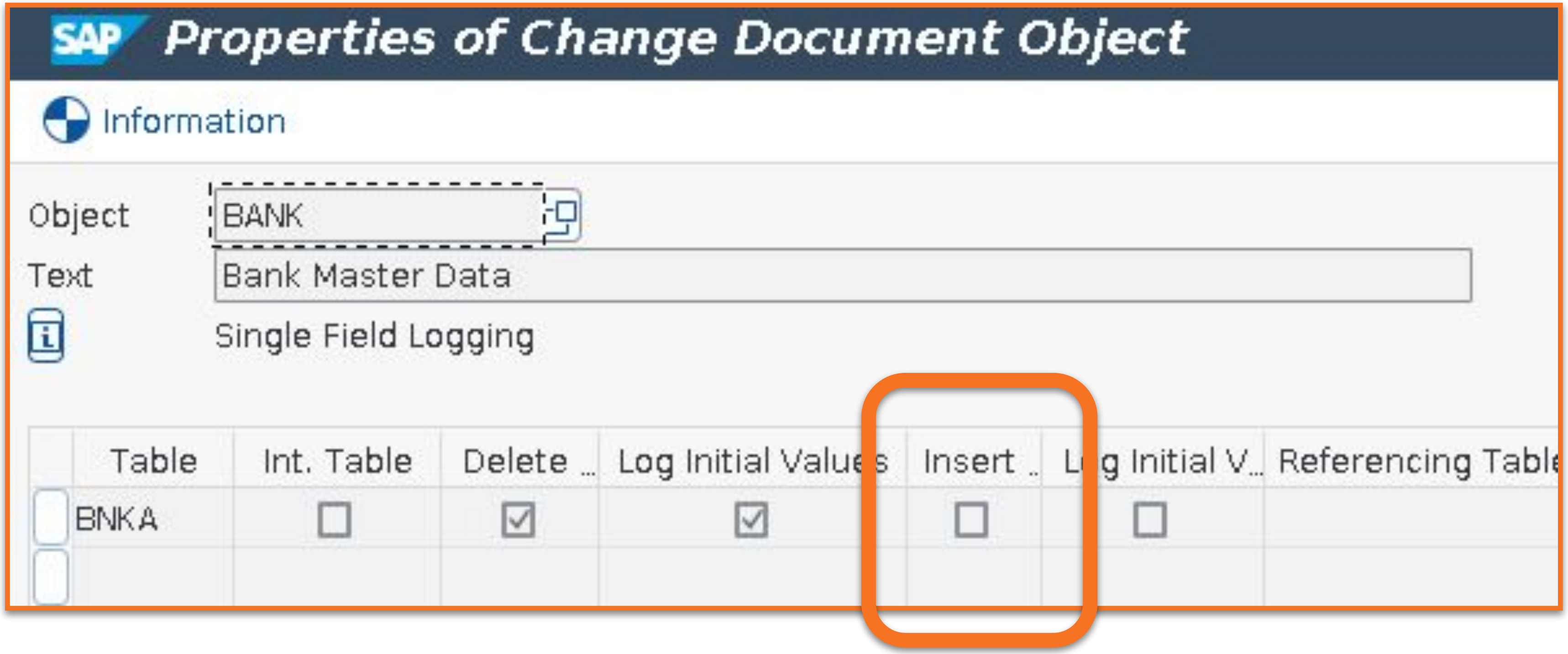
Object BANK

Text Bank Master Data

Single Field Logging

Table	Int. Table	Delete ...	Log Initial Values	Insert ...	Log Initial V...	Referencing Tabl
BNKA	□	☑	☑	□	□	

ABAP - Table - Change Documents



Properties of Change Document Object

Object BANK

Text Bank Master Data

Single Field Logging

Table	Int. Table	Delete ...	Log Initial Values	Insert ...	Log Initial V...	Referencing Table
BNKA	□	☑	☑	□	□	

ABAP - Table - Change Documents

- 800+ Objects logged by default
- Example :

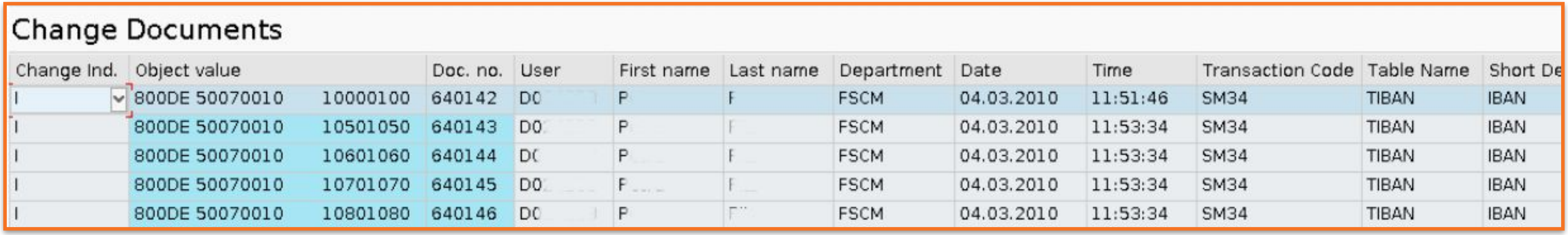
Table	**Short description**
BNKA	Bank master record
TIBAN	IBAN
CCARD	Payment Card Master
LOYD_CRD_CARD	Cards table
BUT0BANK	Business Partner: Bank Data

ABAP - Table - Change Documents

- Tables that **NOT** logged by default
- Example :

Table	**Short description**
LFBK	Vendor Master (bank Details)
PAYR	Payment Medium File
KNBK	Customer Master (bank Details)
T012K	House bank Accounts
FEBAN	Transfer Structure: Requisition to Update Program
T012	House banks
FEBKO	Electronic bank Statement Header Records
P0009	HR Master Record: Infotype 0009 (bank Details)
PC209	Payroll Results: bank transfers
…	…

ABAP - Table - Change Documents *

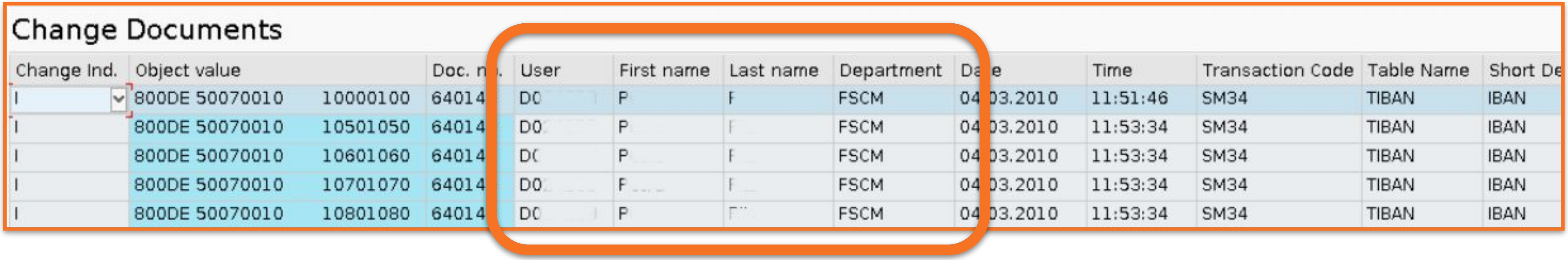


Change Documents

Change Ind.	Object value	Doc. no.	User	First name	Last name	Department	Date	Time	Transaction Code	Table Name	Short De
I	800DE 50070010 10000100	640142	D0	P	F	FSCM	04.03.2010	11:51:46	SM34	TIBAN	IBAN
I	800DE 50070010 10501050	640143	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10601060	640144	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10701070	640145	D0	F	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10801080	640146	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

ABAP - Table - Change Documents *



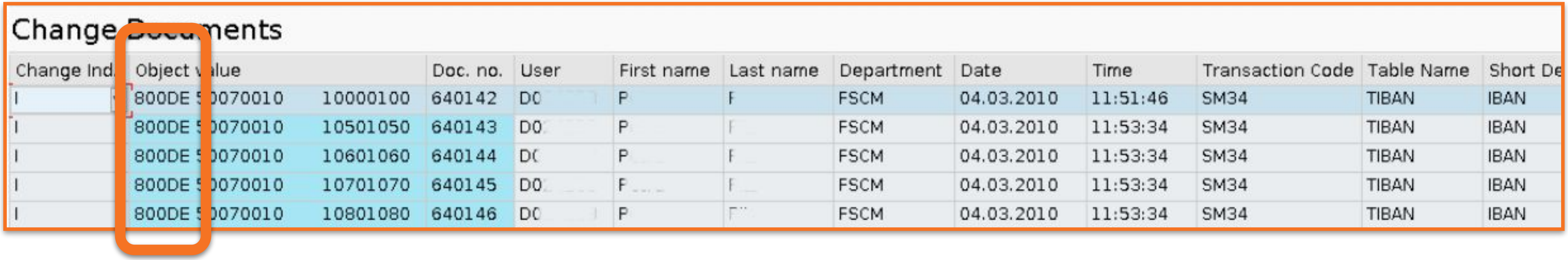
Change Documents

Change Ind.	Object value	Doc. no.	User	First name	Last name	Department	Date	Time	Transaction Code	Table Name	Short De
I	800DE 50070010 10000100	64014	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:51:46	SM34	TIBAN	IBAN
I	800DE 50070010 10501050	64014	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10601060	64014	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10701070	64014	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10801080	64014	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN

User D0xx from FSCM department

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

ABAP - Table - Change Documents *



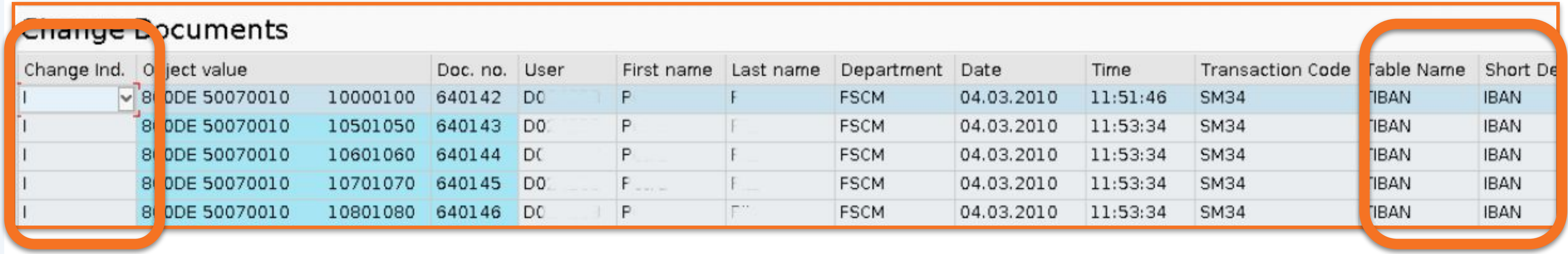
Change Documents

Change Ind.	Object value		Doc. no.	User	First name	Last name	Department	Date	Time	Transaction Code	Table Name	Short De
I	800DE 5[illegible]070010	10000100	640142	D0	P	F	FSCM	04.03.2010	11:51:46	SM34	TIBAN	IBAN
I	800DE 5[illegible]070010	10501050	640143	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 5[illegible]070010	10601060	640144	D(	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 5[illegible]070010	10701070	640145	D0	F	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 5[illegible]070010	10801080	640146	D(	P	F	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN

User D0xx from FSCM department on mandant 800

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

ABAP - Table - Change Documents *



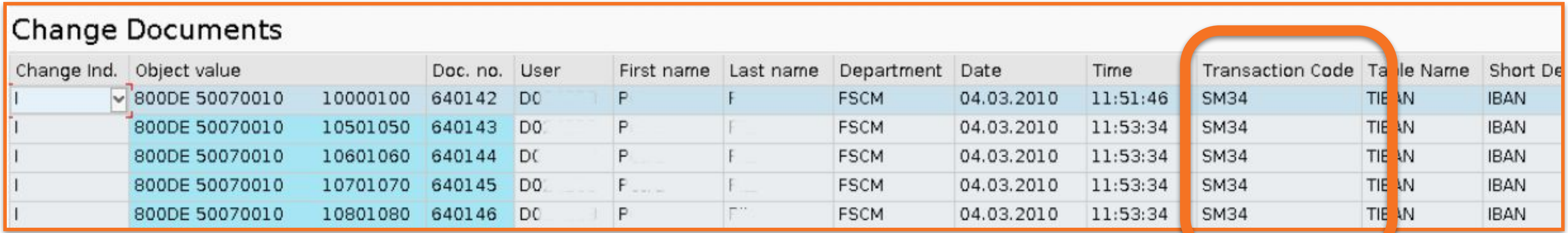
Change Documents

Change Ind.	Object value	Doc. no.	User	First name	Last name	Department	Date	Time	Transaction Code	Table Name	Short De
I	800DE 50070010 10000100	640142	D0	P	F	FSCM	04.03.2010	11:51:46	SM34	IBAN	IBAN
I	800DE 50070010 10501050	640143	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	IBAN	IBAN
I	800DE 50070010 10601060	640144	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	IBAN	IBAN
I	800DE 50070010 10701070	640145	D0	F	F	FSCM	04.03.2010	11:53:34	SM34	IBAN	IBAN
I	800DE 50070010 10801080	640146	D0	P	F	FSCM	04.03.2010	11:53:34	SM34	IBAN	IBAN

User D0xx from FSCM department on mandant 800, insert 5 new IBAN

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

ABAP - Table - Change Documents *



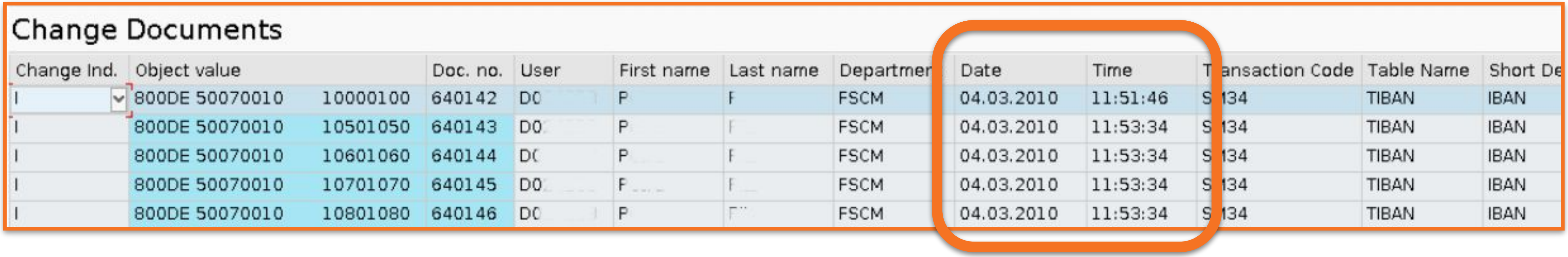
Change Documents

Change Ind.	Object value		Doc. no.	User	First name	Last name	Department	Date	Time	Transaction Code	Table Name	Short De
I	800DE 50070010	10000100	640142	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:51:46	SM34	TIBAN	IBAN
I	800DE 50070010	10501050	640143	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010	10601060	640144	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010	10701070	640145	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010	10801080	640146	D0[redacted]	P[redacted]	F[redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN

User D0xx from FSCM department on mandant 800, insert 5 new IBAN using SM34 transaction

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

ABAP - Table - Change Documents *



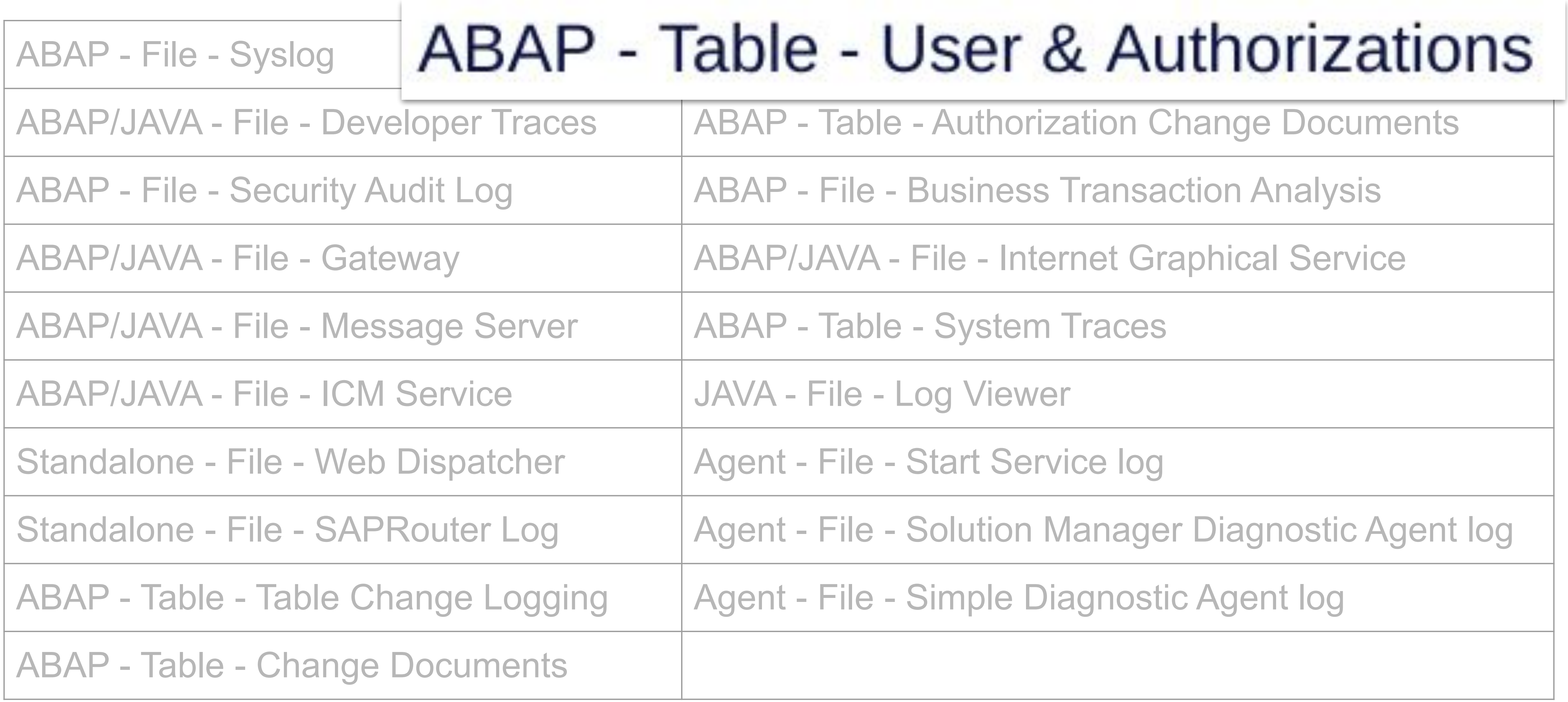
Change Documents

Change Ind.	Object value	Doc. no.	User	First name	Last name	Departmen	Date	Time	Transaction Code	Table Name	Short De
I	800DE 50070010 10000100	640142	D0 [redacted]	P [redacted]	F [redacted]	FSCM	04.03.2010	11:51:46	SM34	TIBAN	IBAN
I	800DE 50070010 10501050	640143	D0 [redacted]	P [redacted]	F [redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10601060	640144	D0 [redacted]	P [redacted]	F [redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10701070	640145	D0 [redacted]	F [redacted]	F [redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN
I	800DE 50070010 10801080	640146	D0 [redacted]	P [redacted]	F [redacted]	FSCM	04.03.2010	11:53:34	SM34	TIBAN	IBAN

User D0xx from FSCM department on mandant 800, insert 5 new IBAN using SM34 transaction just before leave to lunch the 4th March 2010.

* Fake data from SAP IDES DEMO system : https://wiki.scn.sap.com/wiki/display/HOME/IDES

SAP Data Sources



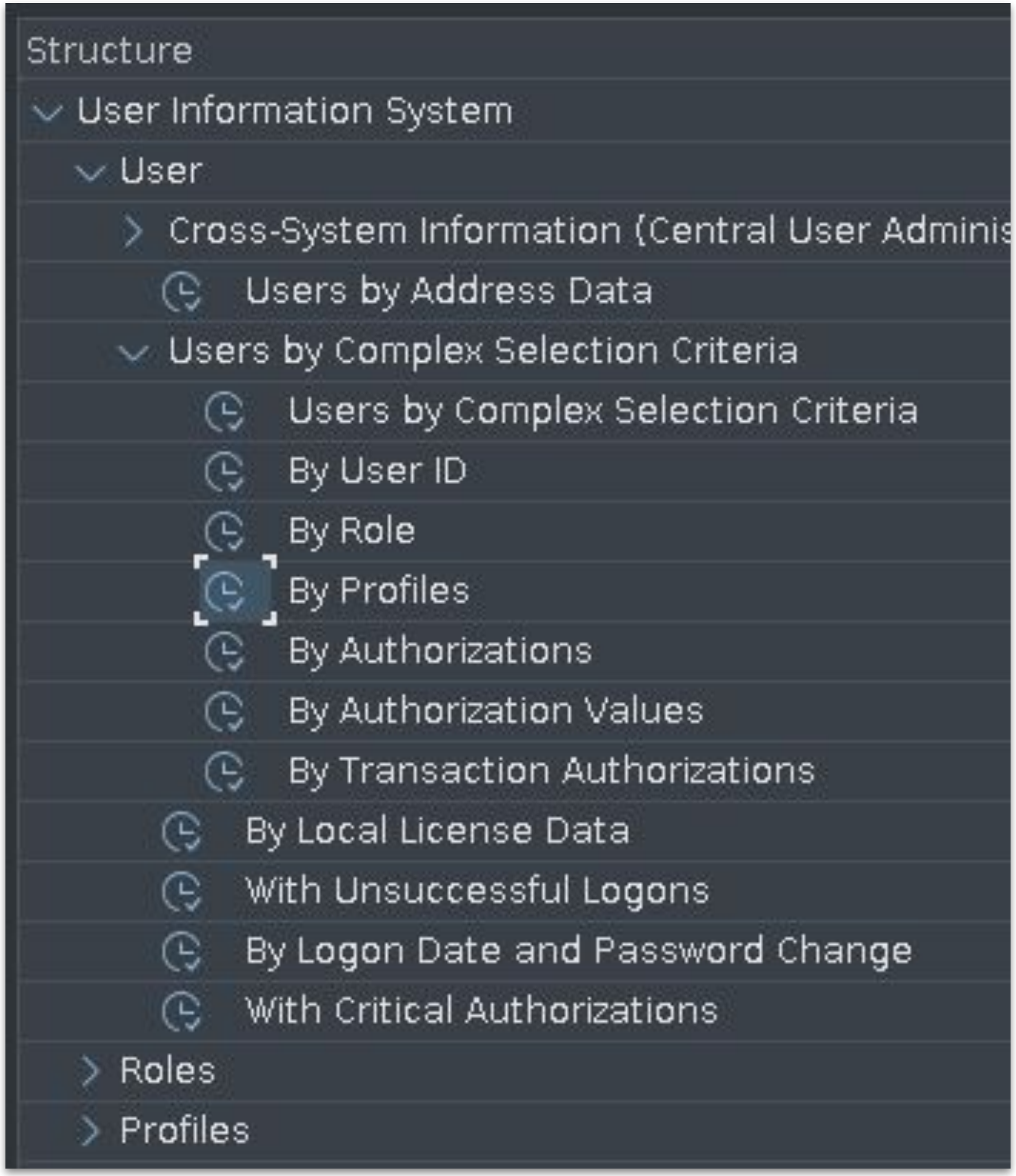
ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

ABAP - Table - User & Authorizations

- User auditing and monitoring swiss-knife

ABAP - Table - User & Authorizations

- User auditing and monitoring swiss-knife



Structure

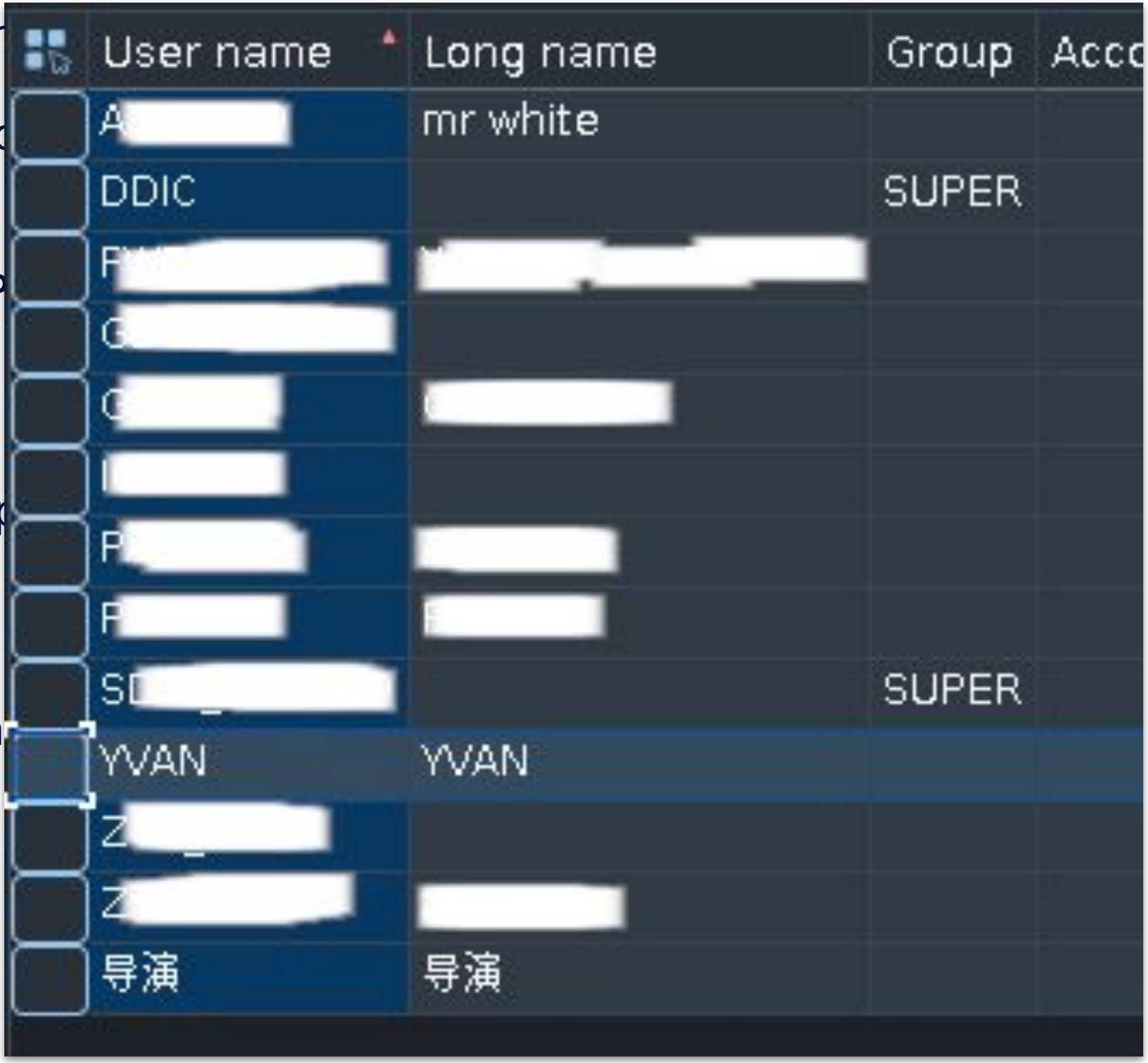
- User Information System
  - User
    - Cross-System Information (Central User Adminis
    - Users by Address Data
    - Users by Complex Selection Criteria
      - Users by Complex Selection Criteria
      - By User ID
      - By Role
      - By Profiles
      - By Authorizations
      - By Authorization Values
      - By Transaction Authorizations
    - By Local License Data
    - With Unsuccessful Logons
    - By Logon Date and Password Change
    - With Critical Authorizations
  - Roles
  - Profiles

ABAP - Table - User & Authorizations

- User auditing and monitoring swiss-knife
- Searching for accounts…
  - … with SAP_ALL profile
  - … that may start any programs
  - … with the privileges to modify sensitive tables
  - … that may execute OS command
  - … with high privileged reference user

ABAP - Table - User & Authorizations

- User auditing ar
- Searching for ac
  - … with SAP
  - … that may
  - … with the p
  - … that may
  - … with high



User name	Long name	Group	Acco
[redacted]	mr white		
DDIC		SUPER	
[redacted]	[redacted]		
[redacted]			
[redacted]	[redacted]		
[redacted]			
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]		SUPER	
YVAN	YVAN		
[redacted]			
[redacted]	[redacted]		
导演	导演		

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA - File - ICM Service	JAVA - File - Log Viewer
Standalone - File - Web Dispatcher	Agent - File - Start Service log
Standalone - File - SAPRouter Log	Agent - File - Solution Manager Diagnostic Agent log
ABAP - Table - Table Change Logging	Agent - File - Simple Diagnostic Agent log
ABAP - Table - Change Documents	

JAVA - File - Log Viewer

- Huge effort to centralize logs and trace files

JAVA - File - Log Viewer

- Huge effort to centralize logs and trace files

- Performing forensic analysis on SAP Netweaver JAVA ?
  Rapidly ask for a full backup of this directory and sub-directories!

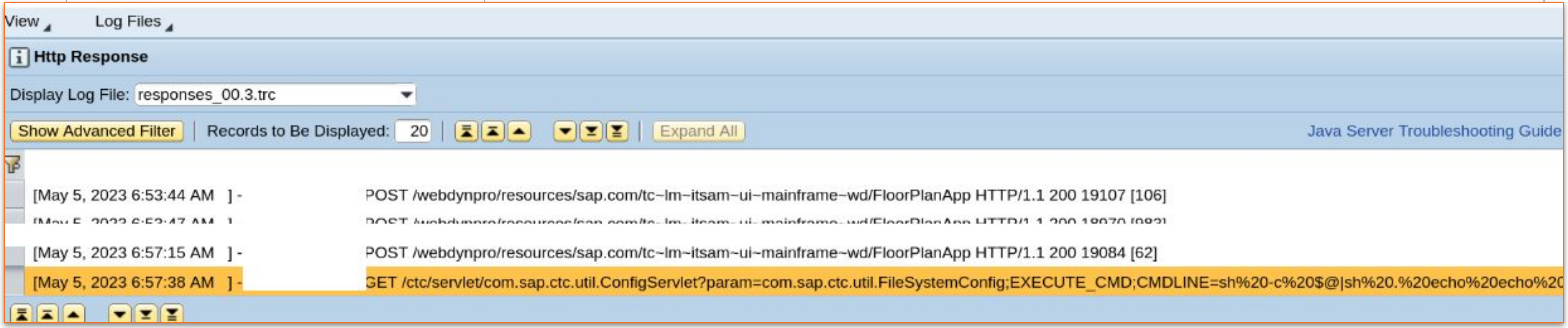
/usr/sap/<SID>/J<Instance_number>/j2ee/cluster/server<NodeNumber>/log

JAVA - File - Log Viewer

View name	Description
Authentication Logs	Logs that give information about logging activities of users
Developer Traces	Main trace records written in defaultTrace.xx.trc file
HTTP Response	HTTP formatted log records written in the responses.trc file
SAP Logs	Log records from all log files (except for defaultTrace.xx.trc)
Security Log	Log written in security* files
System Logs and Traces	Log and trace records, including defaulTrace.xx.trc
Uploaded Log Files	External logs uploaded

JAVA - File - Log Viewer

View name	Description
Authentication Logs	Logs that give information about logging activities of users
Developer Traces	Main trace records written in defaultTrace.xx.trc file
HTTP Response	**HTTP formatted log records written in the responses.trc file**



Display Log File: responses_00.3.trc

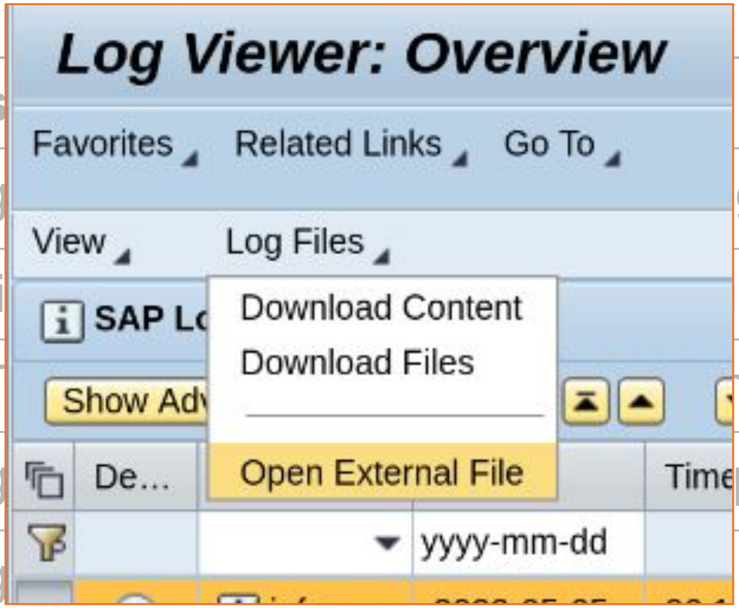
Records to Be Displayed: 20

```
[May 5, 2023 6:53:44 AM   ] -             POST /webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp HTTP/1.1 200 19107 [106]
[May 5, 2023 6:53:47 AM   ] -             POST /webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp HTTP/1.1 200 18970 [983]
[May 5, 2023 6:57:15 AM   ] -             POST /webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp HTTP/1.1 200 19084 [62]
[May 5, 2023 6:57:38 AM   ] -             GET /ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=sh%20-c%20$@|sh%20.%20echo%20echo%20
```

Old CTC RCE attack pattern CVE-2010-5326

JAVA - File - Log Viewer

View name	Des
Authentication Logs	Log gging activities of users
Developer Traces	Mai ltTrace.xx.trc file
HTTP Response	HT n in the responses.trc file
SAP Logs	Log pt for defaultTrace.xx.trc)
Security Log	Log
System Logs and Traces	Log and trace records, including defaulTrace.xx.trc
Uploaded Log Files	**External logs uploaded**



JAVA - File - Log Viewer

- Huge effort to centralize logs and trace files
- Performing forensic analysis on SAP Netweaver JAVA ?
  Rapidly ask for a full backup of this directory and sub-directories!

/usr/sap/<SID>/J<Instance_number>/j2ee/cluster/server<NodeNumber>/log

JAVA - File - Log Viewer

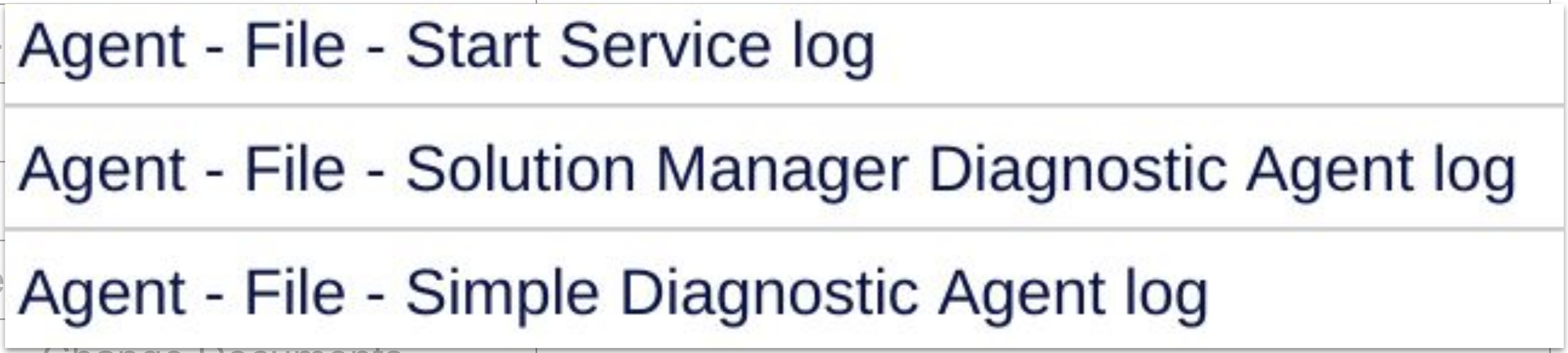
- Huge effort to centralize logs and trace files
- Performing forensic analysis on SAP Netweaver JAVA ?
  Rapidly ask for a full backup of this directory and sub-directories!

rm -rf

/usr/sap/<SID>/J<Instance_number>/j2ee/cluster/server<NodeNumber>/log

SAP Data Sources

ABAP - File - Syslog	ABAP - Table - User & Authorizations
ABAP/JAVA - File - Developer Traces	ABAP - Table - Authorization Change Documents
ABAP - File - Security Audit Log	ABAP - File - Business Transaction Analysis
ABAP/JAVA - File - Gateway	ABAP/JAVA - File - Internet Graphical Service
ABAP/JAVA - File - Message Server	ABAP - Table - System Traces
ABAP/JAVA -	
Standalone -	
Standalone -	
ABAP - Table	
ABAP - Table - Change Documents	

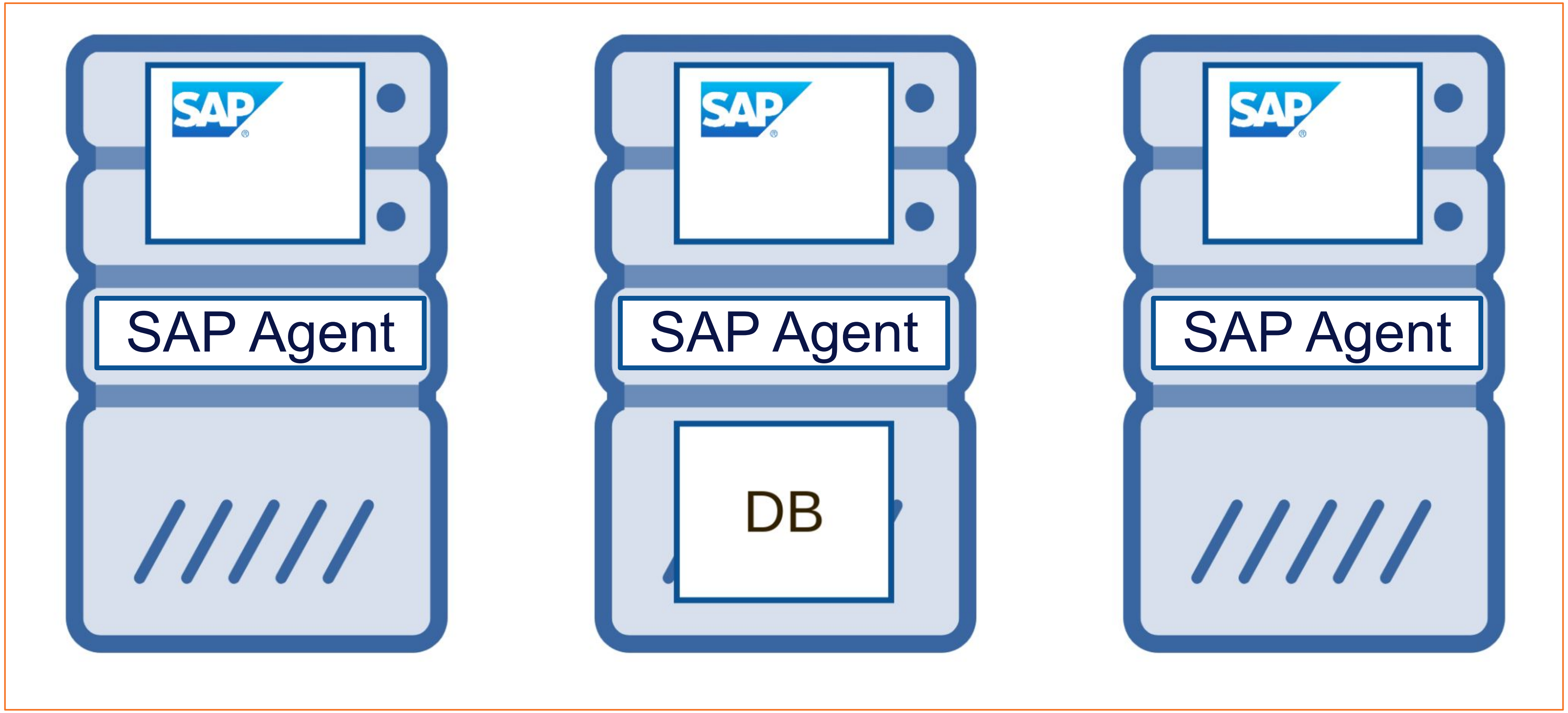


Agent - File - Start Service log

Agent - File - Solution Manager Diagnostic Agent log

Agent - File - Simple Diagnostic Agent log

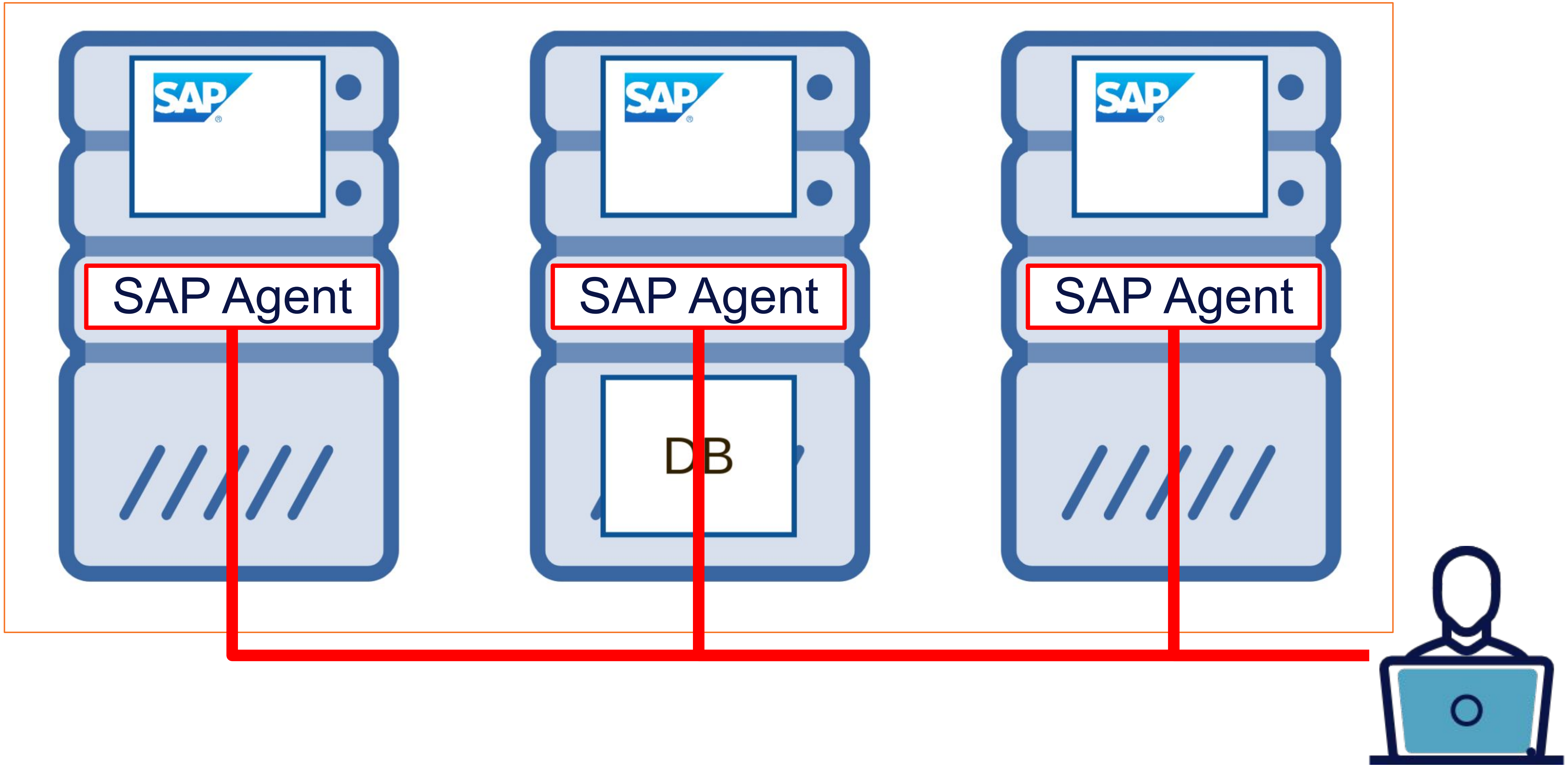
Agent - File - *



Agent - File - *

CVE-2019-0307 Information Disclosure in SAP Diagnostics Agent
CVE-2019-0318 SAP Diagnostic Agent - Credential Exposure Through Log Files
CVE-2019-0330 OS Command Injection vulnerability in SAP Diagnostics Agent
CVE-2020-6198 Missing Authentication check in SAP Diagnostics Agent
CVE-2020-6234 Privilege Escalation in SAP Host Agent
CVE-2020-6236 Privilege Escalation in SAP Landscape Management
CVE-2022-24396 SAP Simple Diagnostic Agent - Missing authentication
CVE-2022-27657 SAP Simple Diagnostic Agent - Arbitrary directory listing
CVE-2022-28774 SAP Host Agent - Credential Exposure Through Log Files
CVE-2023-24523 Privilege Escalation vulnerability in SAP Host Agent

Agent - File - *



AGENDA

0x01 Why SAP Forensic ?

0x02 The White Paper

0x03 SAP Data Sources

0x04 Good to know…

0x05 Closing part

Closing part - SAP Logs Collector

- https://github.com/Onapsis/SAP_Logs_Collector

```
SAP Logs Collector
This script will create an archive file with all SAP logs.

Syntax: ./SAP_Logs_Collector_unix.sh [-d <destination>] [-a <zip|tar>] [-b <SAP Base
directory>] [-h]
Options:
d   Path of the archive file destination. Default [.]
a   Archive tool to use : zip or tar. Default [zip]
b   SAP base directory. Default [/usr/sap]
h   Print this help.
```

Closing part - SAP Logs Collector

- https://github.com/Onapsis/SAP_Logs_Collector

```
NAME
    SAP_Logs_Collector_win.ps1


SYNOPSIS
    Simple SAP logs collector


SYNTAX
    SAP_Logs_Collector_win.ps1 [[-Destination] <String>] [[-SAPBase] <String>]
[<CommonParameters>]


DESCRIPTION
    Collect and compress SAP logs of the current system


RELATED LINKS
    https://www.onapsis.com
```

Closing part - Conclusion

- Very heterogeneous environments
- SAP provides in the standard several tools to perform technical forensic

Closing part - Conclusion

- Very heterogeneous environments
- SAP provides in the standard several tools to perform technical forensic
- Enable necessary logging
- Verify your data sources configuration
- Backup / Export logs to a centralized platform

Closing part - Conclusion

- Very heterogeneous environments
- SAP provides in the standard several tools to perform technical forensic
- Enable necessary logging
- Verify your data sources configuration
- Backup / Export logs to a centralized platform
- If attacker reach enough privileges = auditing not reliable
- Attacker could cover they traces or put false positive
- Don’t blind trust data source

References

1. https://troopers.de/media/filer_public/45/27/4527f0d5-d4ca-40c1-83c6-f0b81bb82518/troopers13-detecting_white-collar_cybercrime_sap_forensics-juan_perez-etchegoyenmariano_nunez.pdf
2. https://confidence-conference.org/archiwum/confidence_11.html
3. https://troopers.de/wp-content/uploads/2013/11/TROOPERS14-Hiding_the_breadcrumbs_Anti-forensics_on_SAP_systems-JuanPerez-Etchegoyen+Will_Vandevanter.pdf
4. https://launchpad.support.sap.com/#/notes/3145046
5. https://launchpad.support.sap.com/#/notes/2902645
6. https://launchpad.support.sap.com/#/notes/2902456
7. https://launchpad.support.sap.com/#/notes/3285757
8. https://launchpad.support.sap.com/#/notes/3158188
9. https://launchpad.support.sap.com/#/notes/2738791
10. https://launchpad.support.sap.com/#/notes/2772266
11. https://launchpad.support.sap.com/#/notes/2808158
12. https://launchpad.support.sap.com/#/notes/2845377
13. https://launchpad.support.sap.com/#/notes/3351410
14. https://go.onapsis.com/threat-report/sap-antiforensics-detecting-whitecollar-cybercrime

THANK YOU

@onapsis

linkedin.com/company/onapsis

ONAPSIS.COM

ONAPSIS