OWASP Core Business Application Security

Security Silverbacks

OWASP

🍴 95

★ 311

Waseem Ajrab, NO MONKEY
Jonathan Stross, Pathlock

OWASP®

Lack of Security Hygiene

Crown Jewels

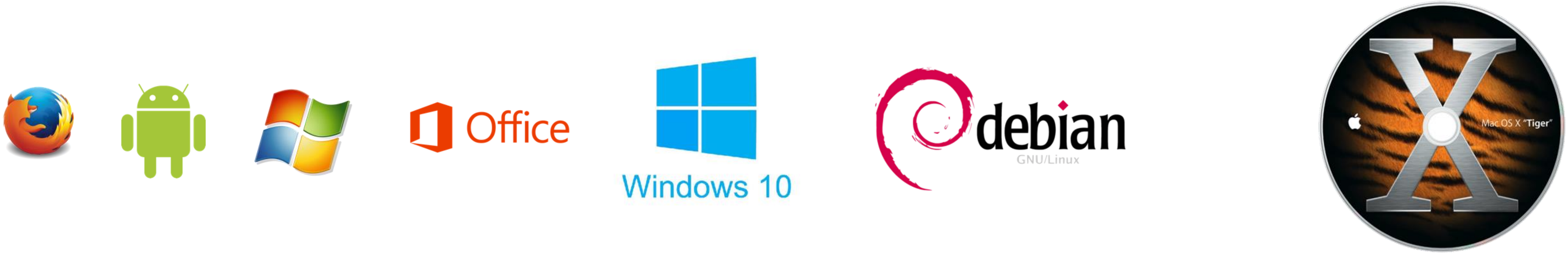
Gold Mine

SAP Complexity…

Is it a blessing or curse?!

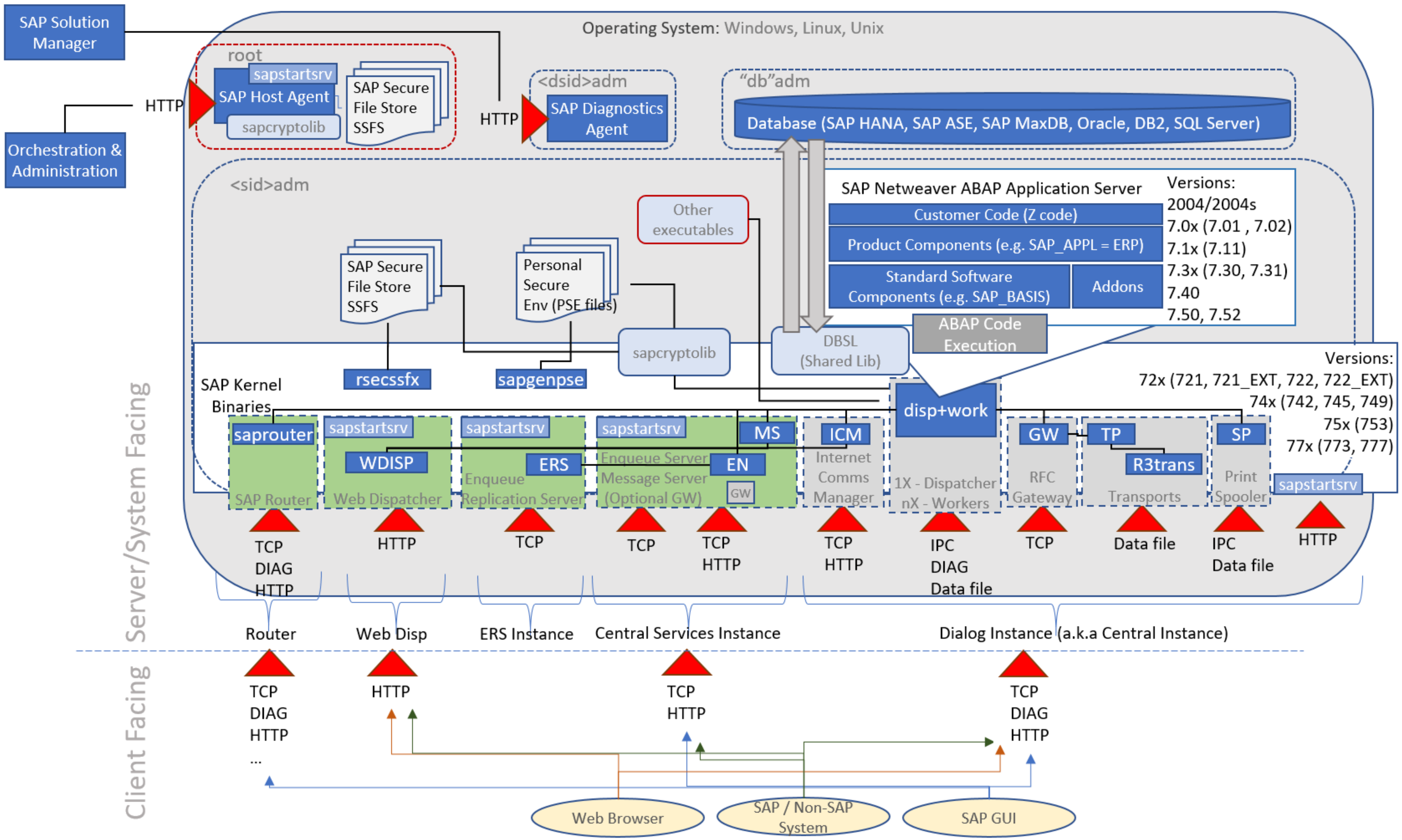
SAP Complexity – Application Level

9,5 | 12 | 40 | 44 | 50 | 67 | 84



SAP Business Suite 319 Million Lines of Code (!)

SAP ERP 6.0 Entry Points



SAP Solution Manager

Orchestration & Administration

HTTP

Operating System: Windows, Linux, Unix

root

sapstartsrv

SAP Host Agent

sapcryptolib

SAP Secure File Store SSFS

HTTP

<dsid>adm

SAP Diagnostics Agent

"db"adm

Database (SAP HANA, SAP ASE, SAP MaxDB, Oracle, DB2, SQL Server)

<sid>adm

Other executables

SAP Netweaver ABAP Application Server

Customer Code (Z code)

Product Components (e.g. SAP_APPL = ERP)

Standard Software Components (e.g. SAP_BASIS)

Addons

ABAP Code Execution

Versions:
2004/2004s
7.0x (7.01 , 7.02)
7.1x (7.11)
7.3x (7.30, 7.31)
7.40
7.50, 7.52

SAP Secure File Store SSFS

Personal Secure Env (PSE files)

sapcryptolib

DBSL (Shared Lib)

rsecssfx

sapgenpse

SAP Kernel Binaries

Versions:
72x (721, 721_EXT, 722, 722_EXT)
74x (742, 745, 749)
75x (753)
77x (773, 777)

saprouter

SAP Router

sapstartsrv

WDISP

Web Dispatcher

sapstartsrv

ERS

Enqueue Replication Server

sapstartsrv

MS

EN

Enqueue Server

Message Server

(Optional GW)

GW

ICM

Internet Comms Manager

disp+work

1X - Dispatcher

nX - Workers

GW

RFC Gateway

TP

R3trans

Transports

SP

Print Spooler

sapstartsrv

TCP
DIAG
HTTP

HTTP

TCP

TCP

TCP
HTTP

TCP
HTTP

IPC
DIAG
Data file

TCP

Data file

IPC
Data file

HTTP

Server/System Facing

Router

Web Disp

ERS Instance

Central Services Instance

Dialog Instance (a.k.a Central Instance)

Client Facing

TCP
DIAG
HTTP
...

HTTP

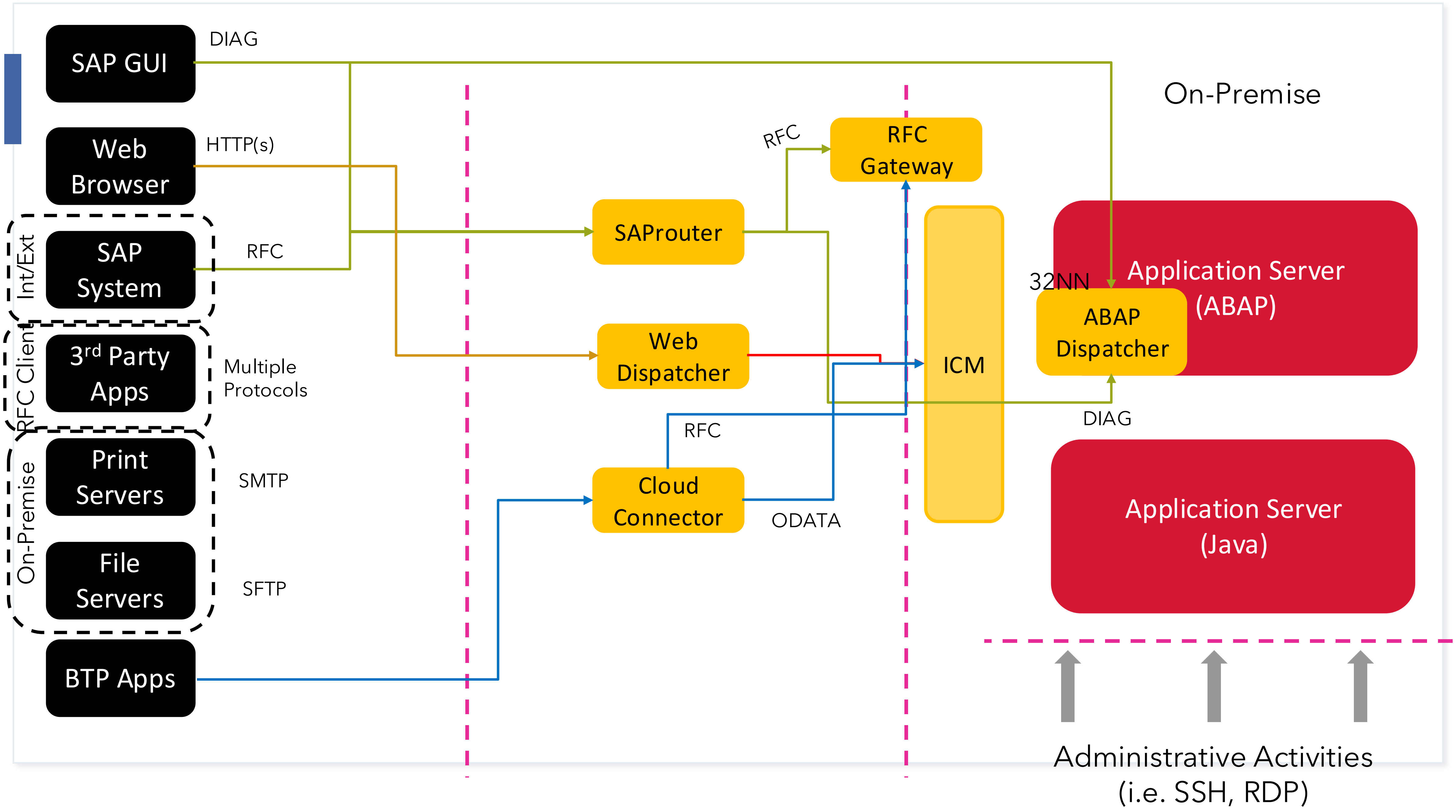
TCP
HTTP

TCP
DIAG
HTTP

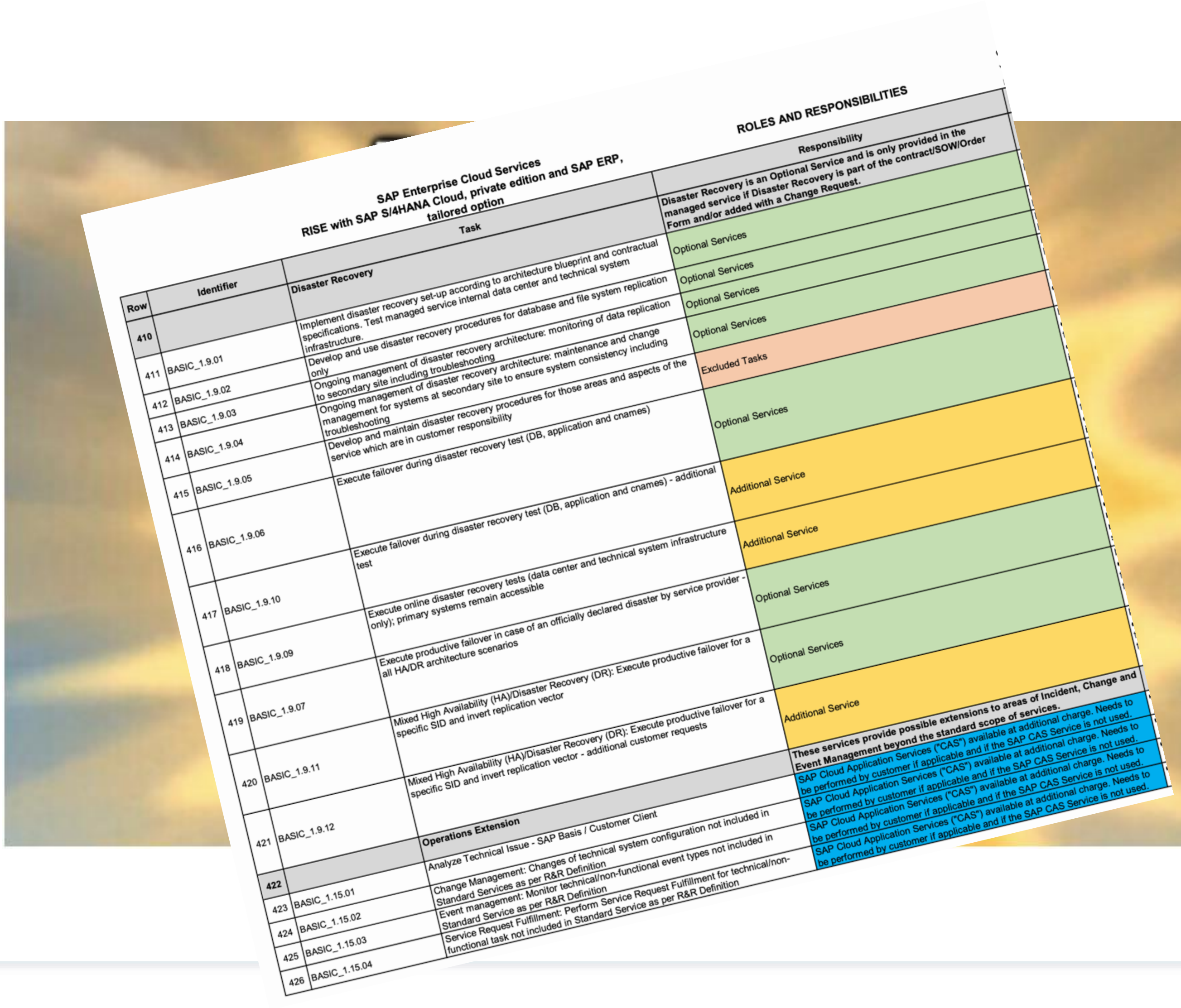
Web Browser

SAP / Non-SAP System

SAP GUI


SAP GUI
DIAG
Web Browser
HTTP(s)
Int/Ext
SAP System
RFC
RFC Client
3rd Party Apps
Multiple Protocols
On-Premise
Print Servers
SMTP
File Servers
SFTP
BTP Apps
SAProuter
RFC
RFC Gateway
Web Dispatcher
RFC
Cloud Connector
ODATA
ICM
On-Premise
32NN
Application Server (ABAP)
ABAP Dispatcher
DIAG
Application Server (Java)
Administrative Activities (i.e. SSH, RDP)

SAP Goes to Cloud

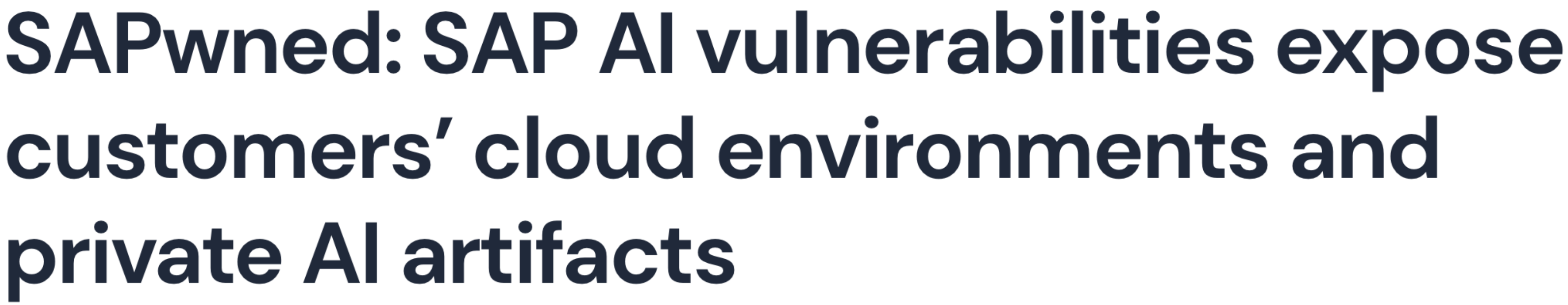


SAP Enterprise Cloud Services
RISE with SAP S/4HANA Cloud, private edition and SAP ERP, tailored option

ROLES AND RESPONSIBILITIES

Row	Identifier	Task	Responsibility
410		**Disaster Recovery**	**Disaster Recovery is an Optional Service and is only provided in the managed service if Disaster Recovery is part of the contract/SOW/Order Form and/or added with a Change Request.**
411	BASIC_1.9.01	Implement disaster recovery set-up according to architecture blueprint and contractual specifications. Test managed service internal data center and technical system infrastructure.	Optional Services
412	BASIC_1.9.02	Develop and use disaster recovery procedures for database and file system replication only	Optional Services
413	BASIC_1.9.03	Ongoing management of disaster recovery architecture: monitoring of data replication to secondary site including troubleshooting	Optional Services
414	BASIC_1.9.04	Ongoing management of disaster recovery architecture: maintenance and change management for systems at secondary site to ensure system consistency including troubleshooting	Optional Services
415	BASIC_1.9.05	Develop and maintain disaster recovery procedures for those areas and aspects of the service which are in customer responsibility	Excluded Tasks
416	BASIC_1.9.06	Execute failover during disaster recovery test (DB, application and cnames)	Optional Services
417	BASIC_1.9.10	Execute failover during disaster recovery test (DB, application and cnames) - additional test	Additional Service
418	BASIC_1.9.09	Execute online disaster recovery tests (data center and technical system infrastructure only); primary systems remain accessible	Additional Service
419	BASIC_1.9.07	Execute productive failover in case of an officially declared disaster by service provider - all HA/DR architecture scenarios	Optional Services
420	BASIC_1.9.11	Mixed High Availability (HA)/Disaster Recovery (DR): Execute productive failover for a specific SID and invert replication vector	Optional Services
421	BASIC_1.9.12	Mixed High Availability (HA)/Disaster Recovery (DR): Execute productive failover for a specific SID and invert replication vector - additional customer requests	Additional Service
422		**Operations Extension**	**These services provide possible extensions to areas of Incident, Change and Event Management beyond the standard scope of services.**
423	BASIC_1.15.01	Analyze Technical Issue - SAP Basis / Customer Client	SAP Cloud Application Services ("CAS") available at additional charge. Needs to be performed by customer if applicable and if the SAP CAS Service is not used.
424	BASIC_1.15.02	Change Management: Changes of technical system configuration not included in Standard Services as per R&R Definition	SAP Cloud Application Services ("CAS") available at additional charge. Needs to be performed by customer if applicable and if the SAP CAS Service is not used.
425	BASIC_1.15.03	Event management: Monitor technical/non-functional event types not included in Standard Service as per R&R Definition	SAP Cloud Application Services ("CAS") available at additional charge. Needs to be performed by customer if applicable and if the SAP CAS Service is not used.
426	BASIC_1.15.04	Service Request Fulfillment: Perform Service Request Fulfillment for technical/non-functional task not included in Standard Service as per R&R Definition	SAP Cloud Application Services ("CAS") available at additional charge. Needs to be performed by customer if applicable and if the SAP CAS Service is not used.

SAP Goes to AI



SAPwned: SAP AI vulnerabilities expose customers’ cloud environments and private AI artifacts

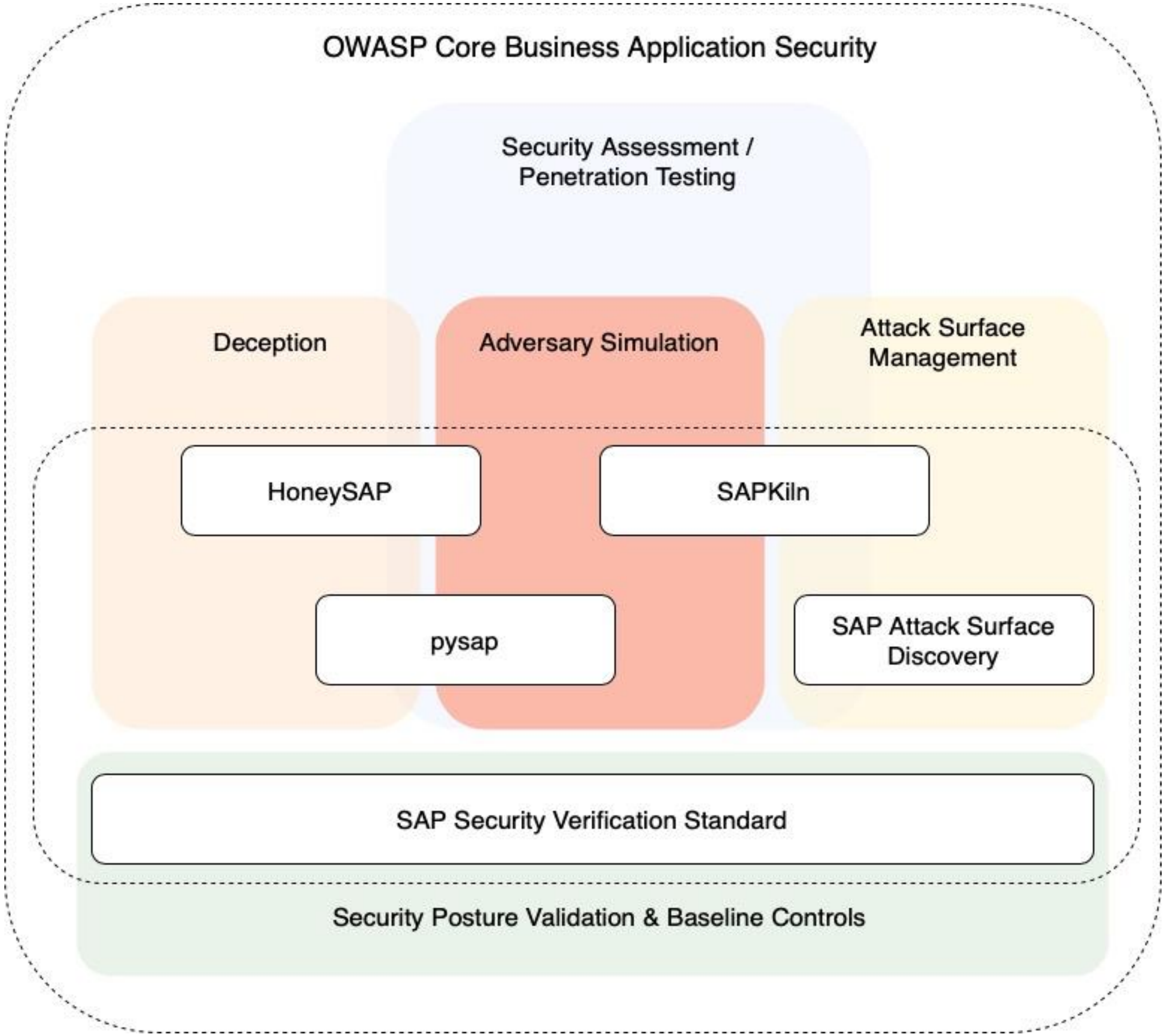
72% of beer production in the world depends on SAP!

SAP Security Myths

- ZERO TRUST
- IAM & AUTHORIZATION
- ENFORCING CONTROLS ONLY ON PRODUCTION
- SAP BASIS TEAM TAKES CARE OF SECURITY
- SAP SYSTEMS ARE ISOLATED AND NOT PUBLISHED
- GERMAN MADE = SECURE BY DEFAULT

Project Goals

- Provide a security standard to secure SAP systems
- Provide the necessary tools to verify security measures
- Provide a single point of trusted security advisors
- Enabling regulators and auditors to assess enterprise business solutions



OWASP Core Business Application Security

Security Assessment / Penetration Testing

Deception

Adversary Simulation

Attack Surface Management

HoneySAP

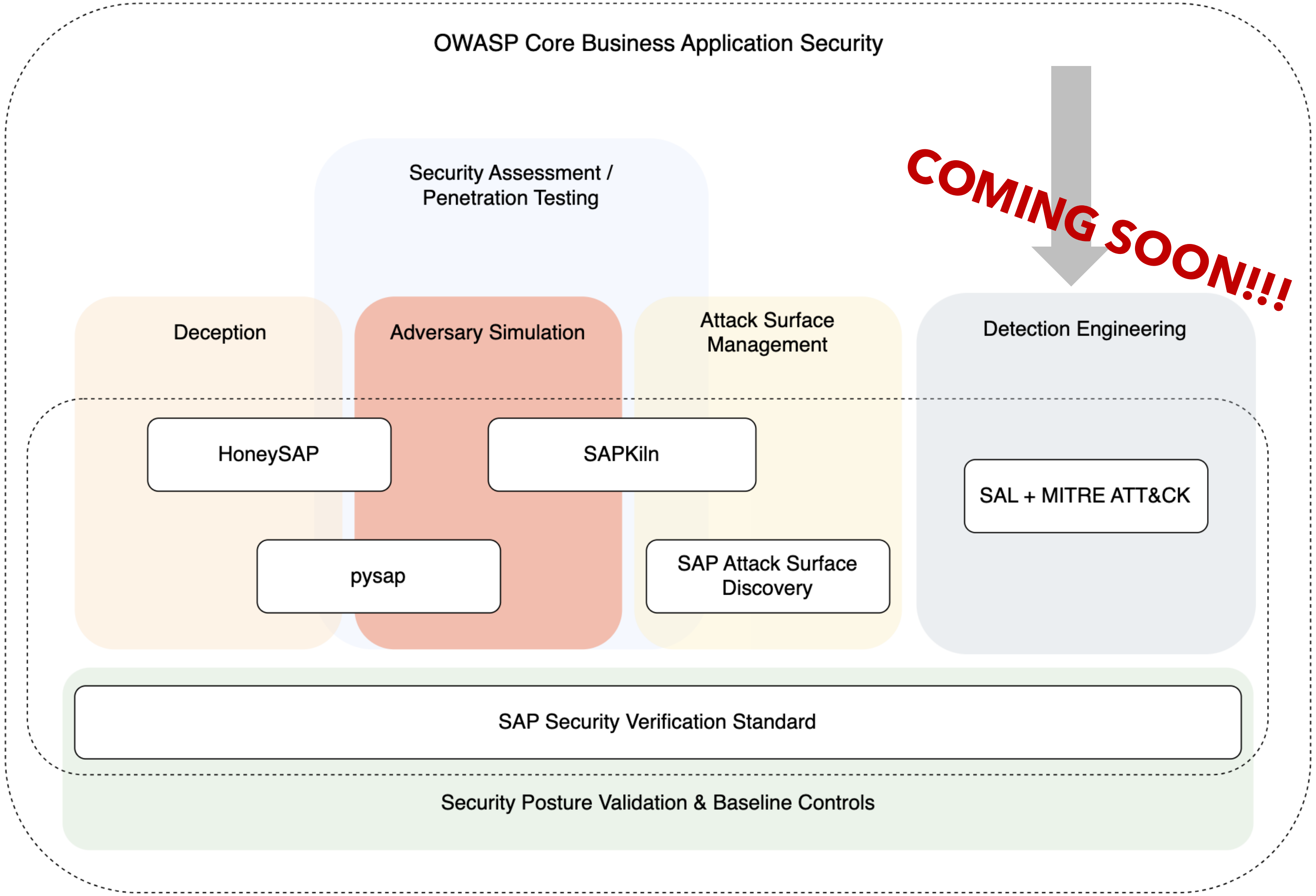
SAPKiln

pysap

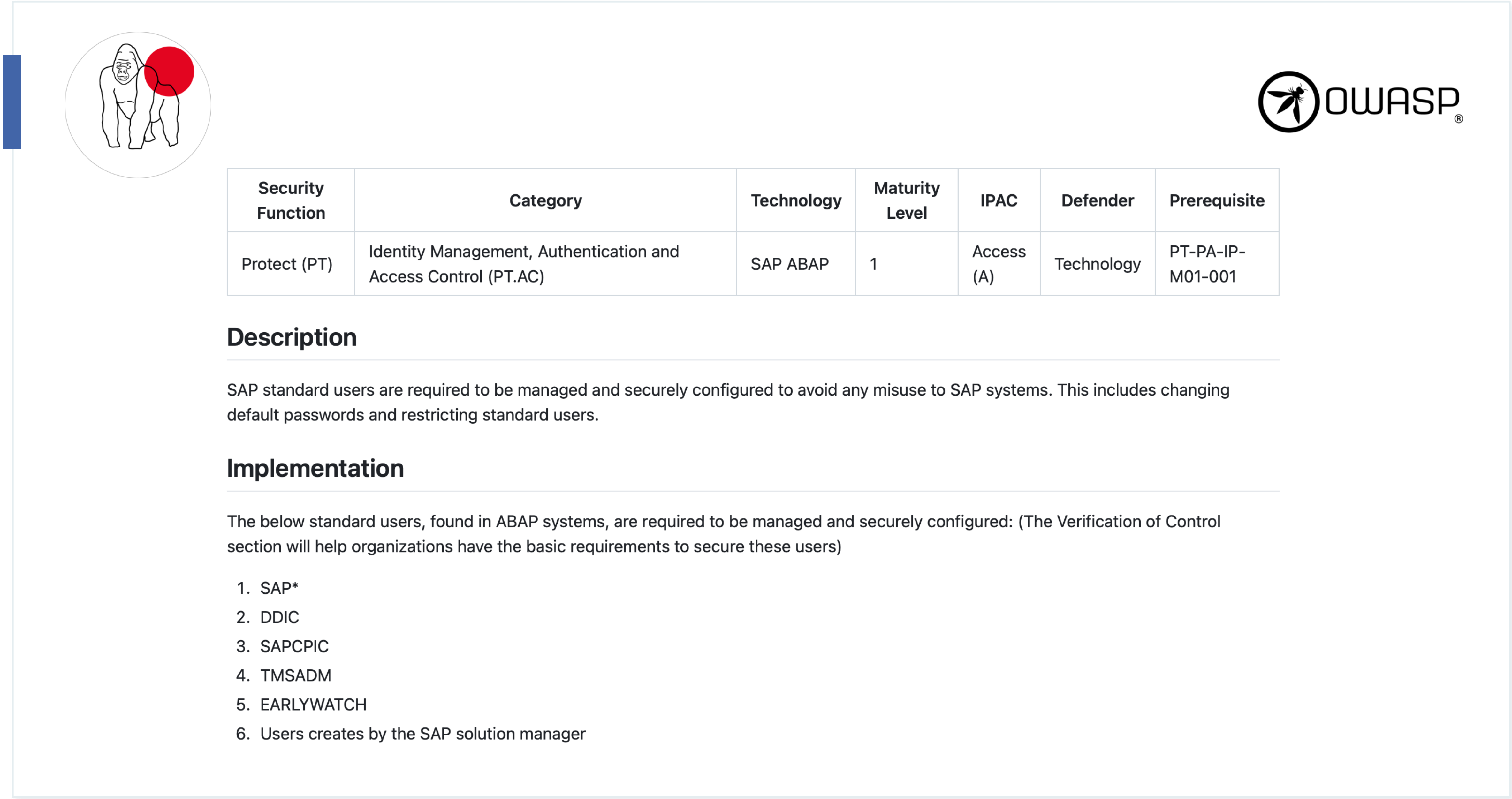
SAP Attack Surface Discovery

SAP Security Verification Standard

Security Posture Validation & Baseline Controls


OWASP Core Business Application Security
Security Assessment / Penetration Testing
COMING SOON!!!
Deception
Adversary Simulation
Attack Surface Management
Detection Engineering
HoneySAP
SAPKiln
SAL + MITRE ATT&CK
pysap
SAP Attack Surface Discovery
SAP Security Verification Standard
Security Posture Validation & Baseline Controls

SAP Security Verification Standard



Security Function	Category	Technology	Maturity Level	IPAC	Defender	Prerequisite
Protect (PT)	Identity Management, Authentication and Access Control (PT.AC)	SAP ABAP	1	Access (A)	Technology	PT-PA-IP-M01-001

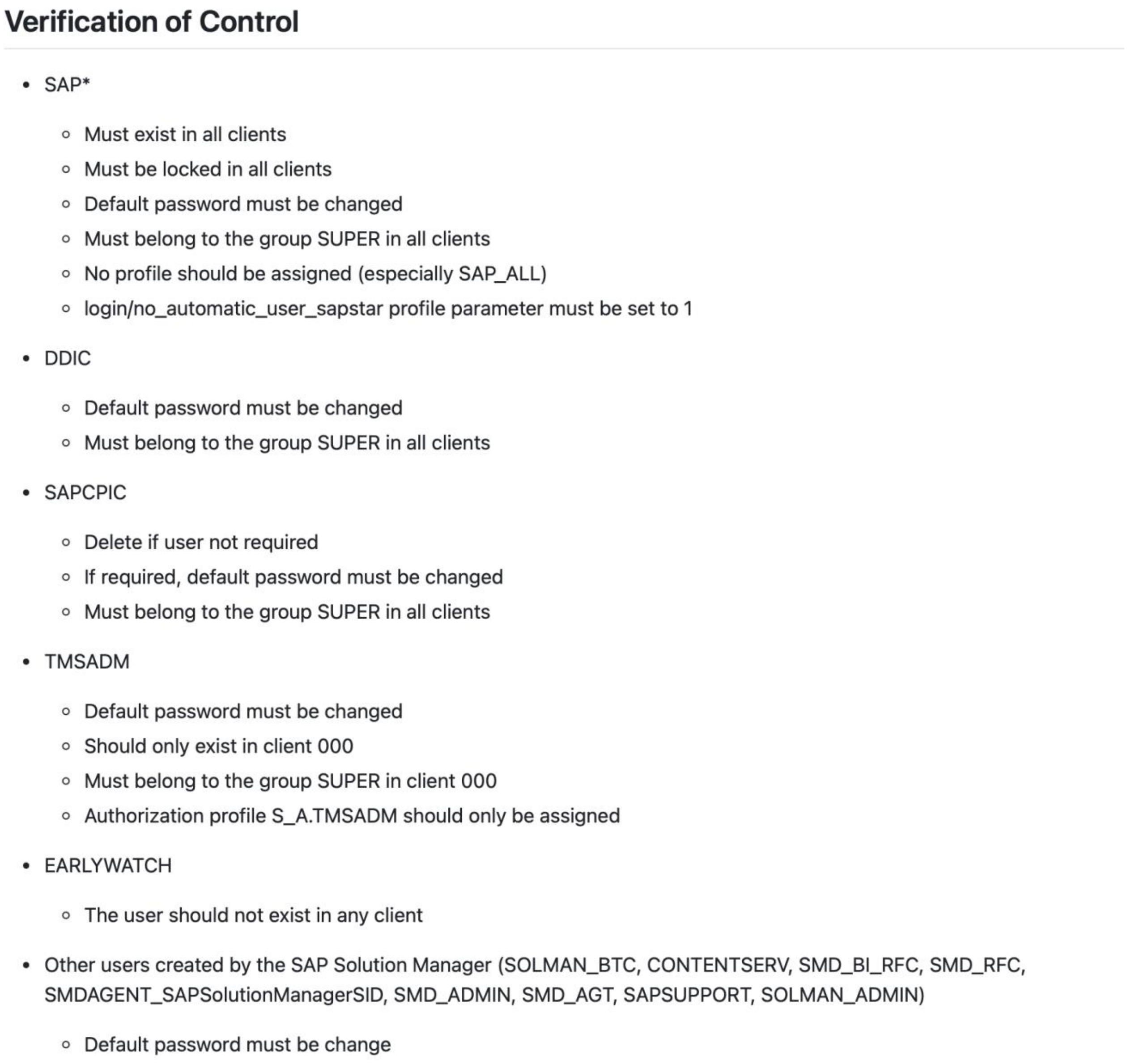
Description

SAP standard users are required to be managed and securely configured to avoid any misuse to SAP systems. This includes changing default passwords and restricting standard users.

Implementation

The below standard users, found in ABAP systems, are required to be managed and securely configured: (The Verification of Control section will help organizations have the basic requirements to secure these users)

1. SAP*
2. DDIC
3. SAPCPIC
4. TMSADM
5. EARLYWATCH
6. Users creates by the SAP solution manager



Verification of Control

- SAP*
  - Must exist in all clients
  - Must be locked in all clients
  - Default password must be changed
  - Must belong to the group SUPER in all clients
  - No profile should be assigned (especially SAP_ALL)
  - login/no_automatic_user_sapstar profile parameter must be set to 1
- DDIC
  - Default password must be changed
  - Must belong to the group SUPER in all clients
- SAPCPIC
  - Delete if user not required
  - If required, default password must be changed
  - Must belong to the group SUPER in all clients
- TMSADM
  - Default password must be changed
  - Should only exist in client 000
  - Must belong to the group SUPER in client 000
  - Authorization profile S_A.TMSADM should only be assigned
- EARLYWATCH
  - The user should not exist in any client
- Other users created by the SAP Solution Manager (SOLMAN_BTC, CONTENTSERV, SMD_BI_RFC, SMD_RFC, SMDAGENT_SAPSolutionManagerSID, SMD_ADMIN, SMD_AGT, SAPSUPPORT, SOLMAN_ADMIN)
  - Default password must be change

Security Function	Category	Technology	Maturity Level	SAP Operational Area	Prerequisite
Detect (DT)	Anomalies and Events (DT.AE)	SAP HANA	2	Access (A)	

Description

HANA audit trails should be written to either the system or tenant database. In the standard configuration, the audit trail parameters can only be changed in the system database.

Implementation

The parameter "default_audit_trail_type" must be set to either the value SYSLOGPROTOCOL or CSTABLE. The value "SYSLOGPROTOCOL" means that the log is written to the system database, while the value "CSTABLE" means that the log is written to the tenant database. This is done in the "global.ini" file in the "auditing configuration" section of the HANA database.

- ALTER SYSTEM ALTER CONFIGURATION ('global.ini', 'SYSTEM') set ('auditing configuration' , 'default_audit_trail_type') = 'SYSLOGPROTOCOL';
- ALTER SYSTEM ALTER CONFIGURATION ('global.ini', 'SYSTEM') set ('auditing configuration' , 'default_audit_trail_type') = 'CSTABLE';

Verification of control

Check that the "default_audit_trail_type" parameter in the "global.ini" file in the "auditing configuration" section is assigned either the value SYSLOGPROTOCOL or CSTABLE.

SAP Security Verification Standard

Support Areas:

- Updating, enhancing, and adding security controls
- Creation of a standard document
- Update Wiki
- Improve and simplify usability
    - Support teams in tracking and monitoring their progress

SAP Attack Surface Discovery

SAP Attack Surface Discovery

- Identification and discovery of SAP services
  - Identify exposed ports
  - Fingerprint services
- Demonstrate the risk of exposed SAP applications
- Provide visibility to non-SAP researchers and other

Where are we?

- Containerized environment
- Nuclei Templates
- Wiki section per service
- Collaboration with hunter.how
- Inclusion of Shodan queries

Services added so far:

- SAPRouter
- SAP Cloud Connector
- SAP Message Server
- SAP Dispatcher
- SAP Web Dispatcher
- SAP Start Service
- SAP RFC Gateway
- SAP Internet Graphics Server
- SAP ASE (DB)

Roadmap

- Add more service i.e. SAP HANA, Web Services, SAP JAVA P4, etc

- Add more tools & references to the services

- Extend intergations with hunter.how

- Create integration with Pysap & SAPKiln projects

Pysap

Features

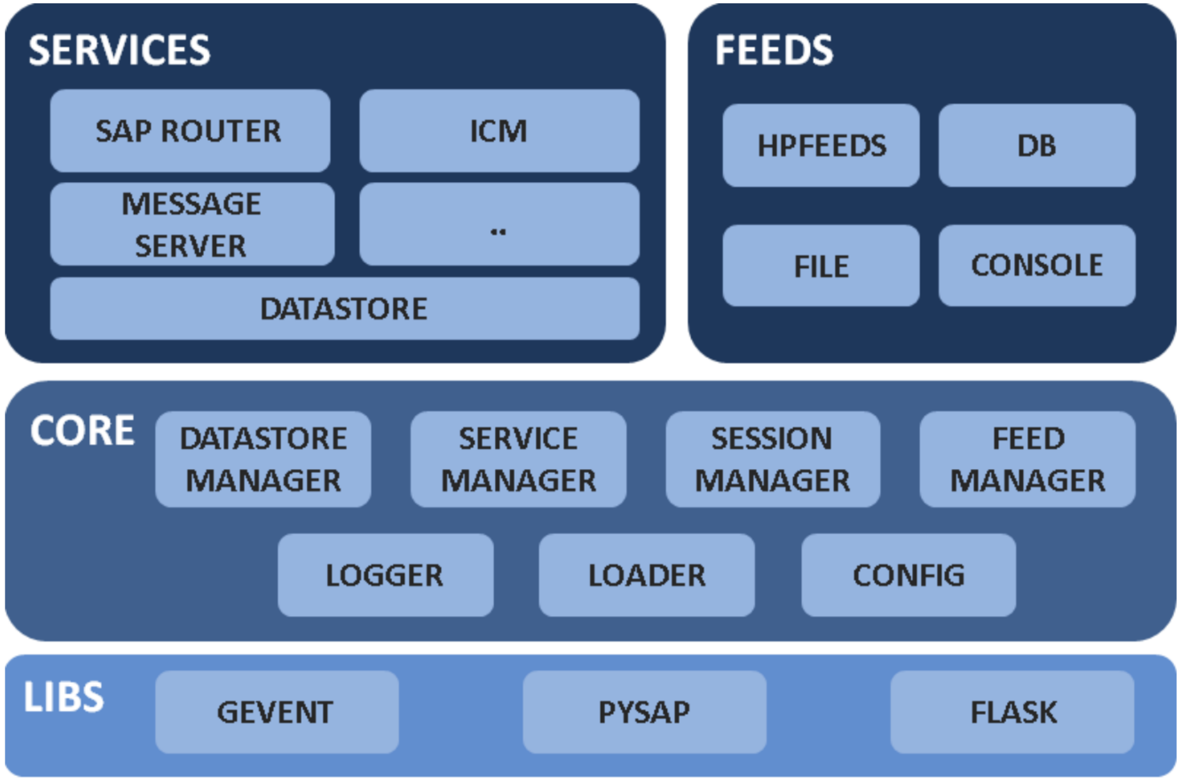
- Dissection and crafting of the following network protocols:
  - SAP Network Interface (NI)
  - SAP Diag
  - SAP Enqueue
  - SAP Router
  - SAP Message Server (MS)
  - SAP Secure Network Connection (SNC)
  - SAP Internet Graphic Server (IGS)
  - SAP Remote Function Call (RFC)
  - SAP HANA SQL Command Network (HDB)

- Client interfaces for handling the following file formats:
  - SAP SAR archive files
  - SAP Personal Security Environment (PSE) files
  - SAP SSO Credential (Credv2) files
  - SAP Secure Storage in File System (SSFS) files
- Library implementing SAP's LZH and LZC compression algorithms.
- Automatic compression/decompression of payloads with SAP's algorithms.
- Client, proxy and server classes implemented for some of the protocols.
- Example scripts to illustrate the use of the different modules and protocols.

HoneySAP

Features

- Low-interaction honeypot for SAP services
- YAML and JSON-based configuration
- Pluggable datastore backend
- Modular services system
- Modular feeds system
- Console logging



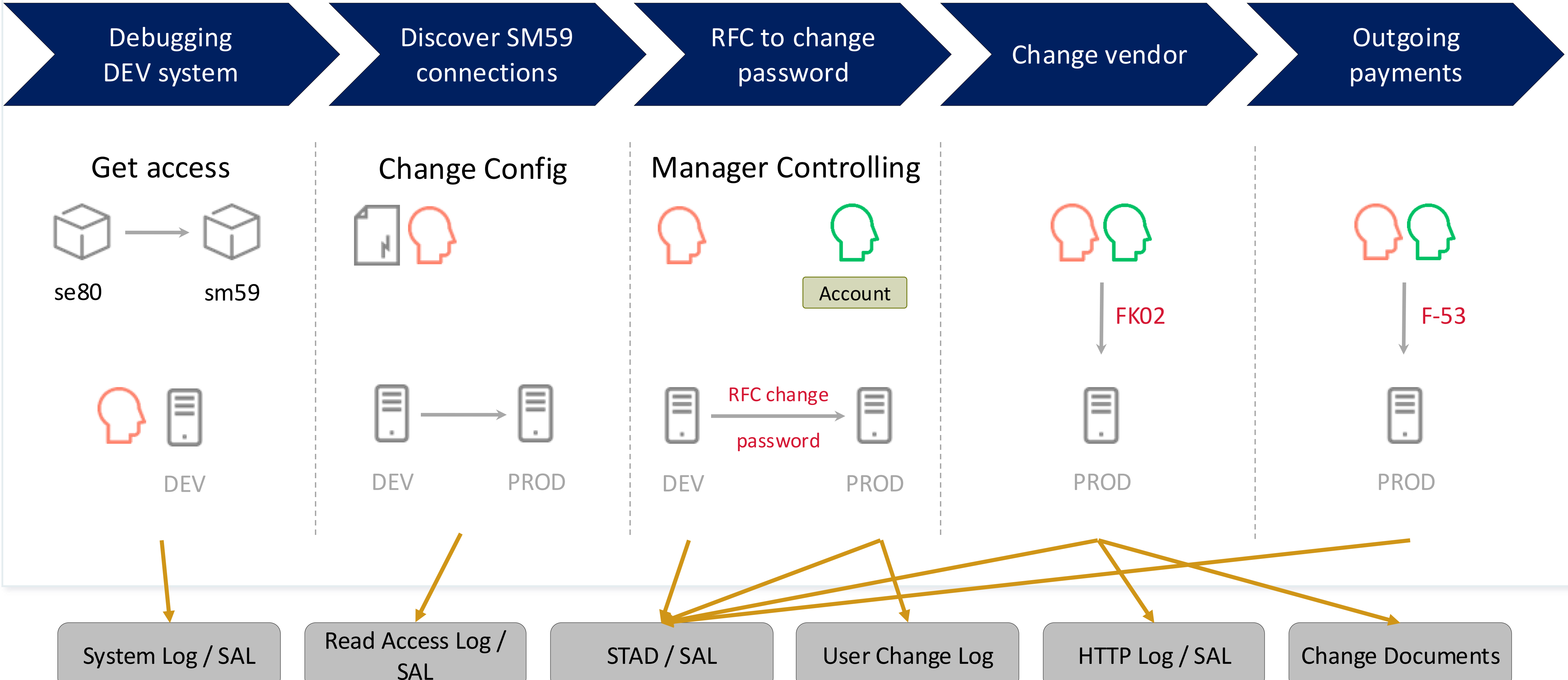
Mitre ATT&CK mapping of SAP SAL*

*SAL: Security Audit Log

SAP and SOC Facts

- SAP Speaks its own language **SAPanese**
- Often times ran by dedicated IT Department
- Often monitored by a SAP Unit but only 9 - 5
- Often no to limited communication between cooperate SOC and SAP Security
- „Holistic Security“ often, sadly, excludes SAP Applications

Detecting Attack



Debugging DEV system

Discover SM59 connections

RFC to change password

Change vendor

Outgoing payments

Get access

Change Config

Manager Controlling

System Log / SAL

Read Access Log / SAL

STAD / SAL

User Change Log

HTTP Log / SAL

Change Documents

Detecting Attack

Debugging DEV system

Disco
con

ange vendor

Outgoing payments

Get access

se80

sm59

DEV

Co

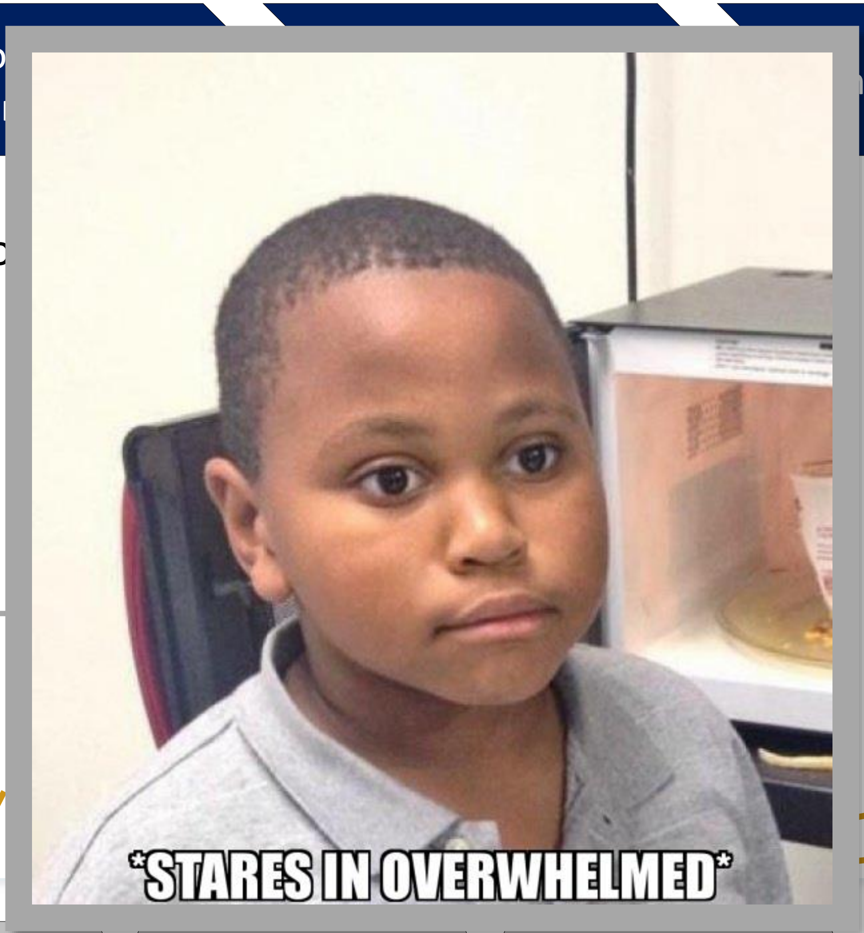
DEV

FK02

PROD

F-53

PROD



System Log / SAL

Read Access Log / SAL

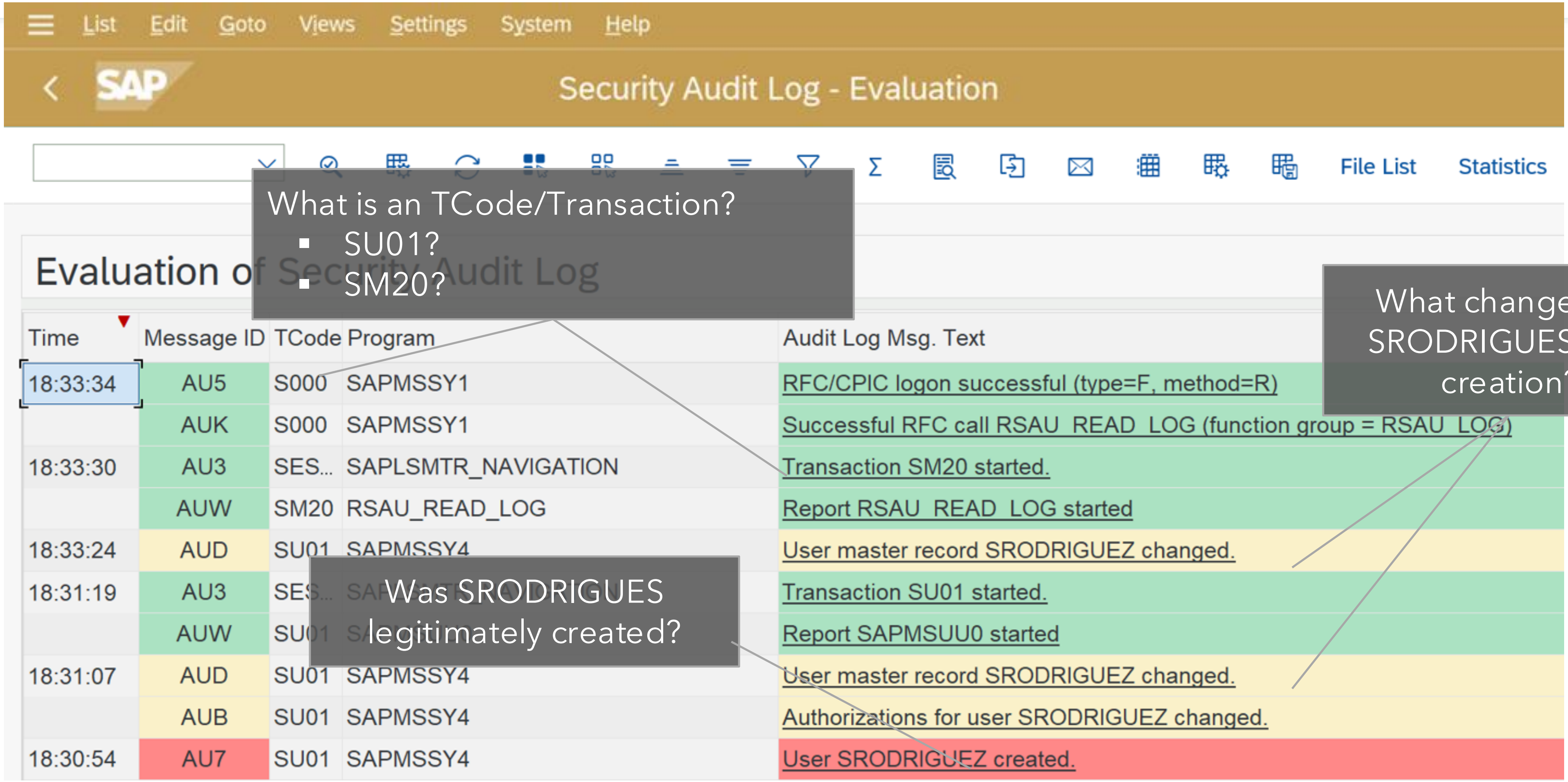
STAD / SAL

User Change Log

HTTP Log / SAL

Change Documents

SAP SAL data out of SOC perspective



Evaluation of Security Audit Log

Time	Message ID	TCode	Program	Audit Log Msg. Text
18:33:34	AU5	S000	SAPMSSY1	RFC/CPIC logon successful (type=F, method=R)
	AUK	S000	SAPMSSY1	Successful RFC call RSAU_READ_LOG (function group = RSAU_LOG)
18:33:30	AU3	SES...	SAPLSMTR_NAVIGATION	Transaction SM20 started.
	AUW	SM20	RSAU_READ_LOG	Report RSAU_READ_LOG started
18:33:24	AUD	SU01	SAPMSSY4	User master record SRODRIGUEZ changed.
18:31:19	AU3	SES...	[illegible]	Transaction SU01 started.
	AUW	SU01	[illegible]	Report SAPMSUU0 started
18:31:07	AUD	SU01	SAPMSSY4	User master record SRODRIGUEZ changed.
	AUB	SU01	SAPMSSY4	Authorizations for user SRODRIGUEZ changed.
18:30:54	AU7	SU01	SAPMSSY4	User SRODRIGUEZ created.

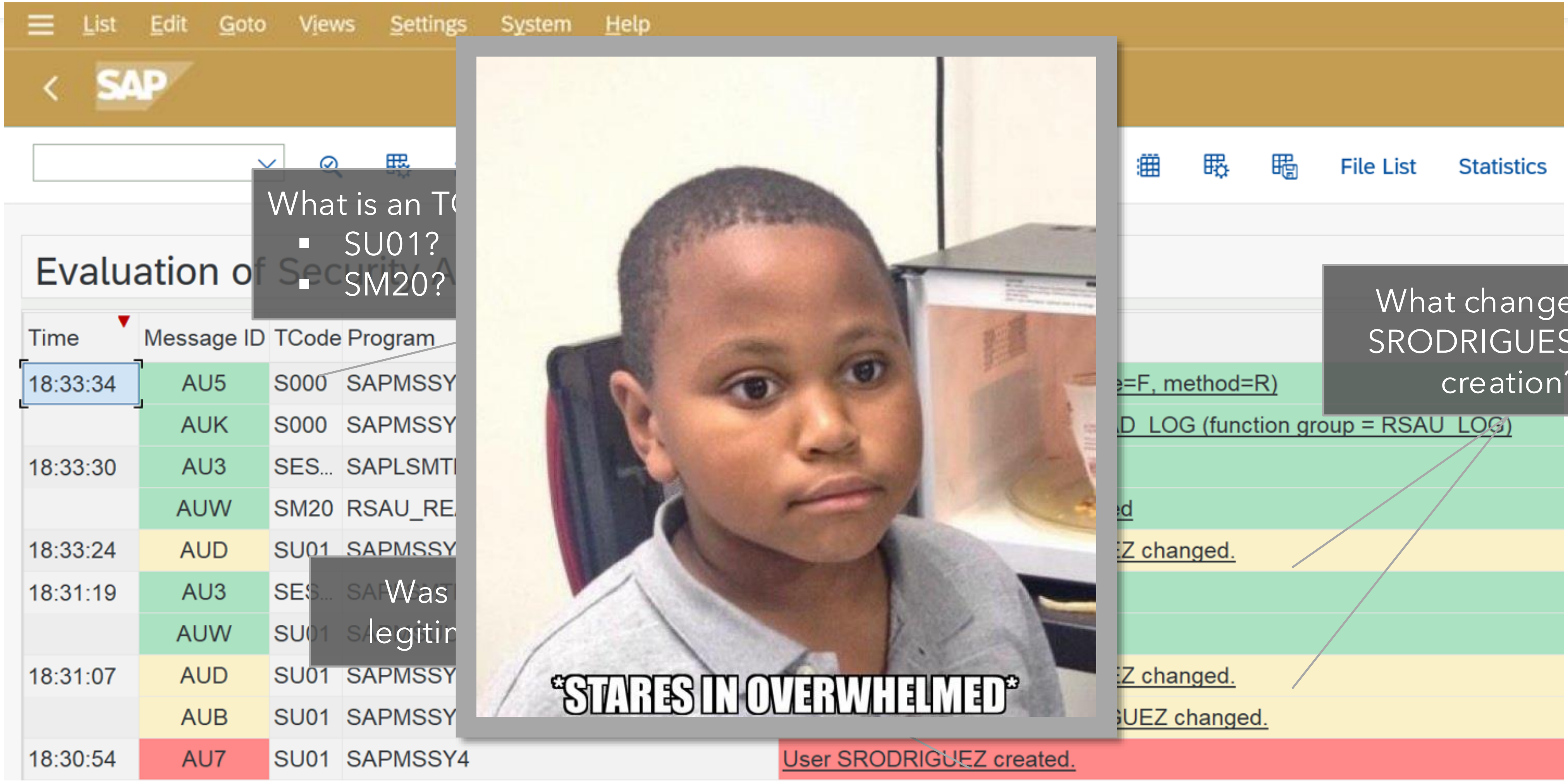
What is an TCode/Transaction?

- SU01?
- SM20?

What changed on SRODRIGUES after creation?

Was SRODRIGUES legitimately created?

SAP SAL data out of SOC perspective



Evaluation of Security A

Time	Message ID	TCode	Program	
18:33:34	AU5	S000	SAPMSSY	e=F, method=R)
	AUK	S000	SAPMSSY	D_LOG (function group = RSAU_LOG)
18:33:30	AU3	SES...	SAPLSMTI	
	AUW	SM20	RSAU_RE	ed
18:33:24	AUD	SU01	SAPMSSY	Z changed.
18:31:19	AU3	SES...	SA	
	AUW	SU01	S	
18:31:07	AUD	SU01	SAPMSSY	Z changed.
	AUB	SU01	SAPMSSY	UEZ changed.
18:30:54	AU7	SU01	SAPMSSY4	User SRODRIGUEZ created.

What is an TC

- SU01?
- SM20?

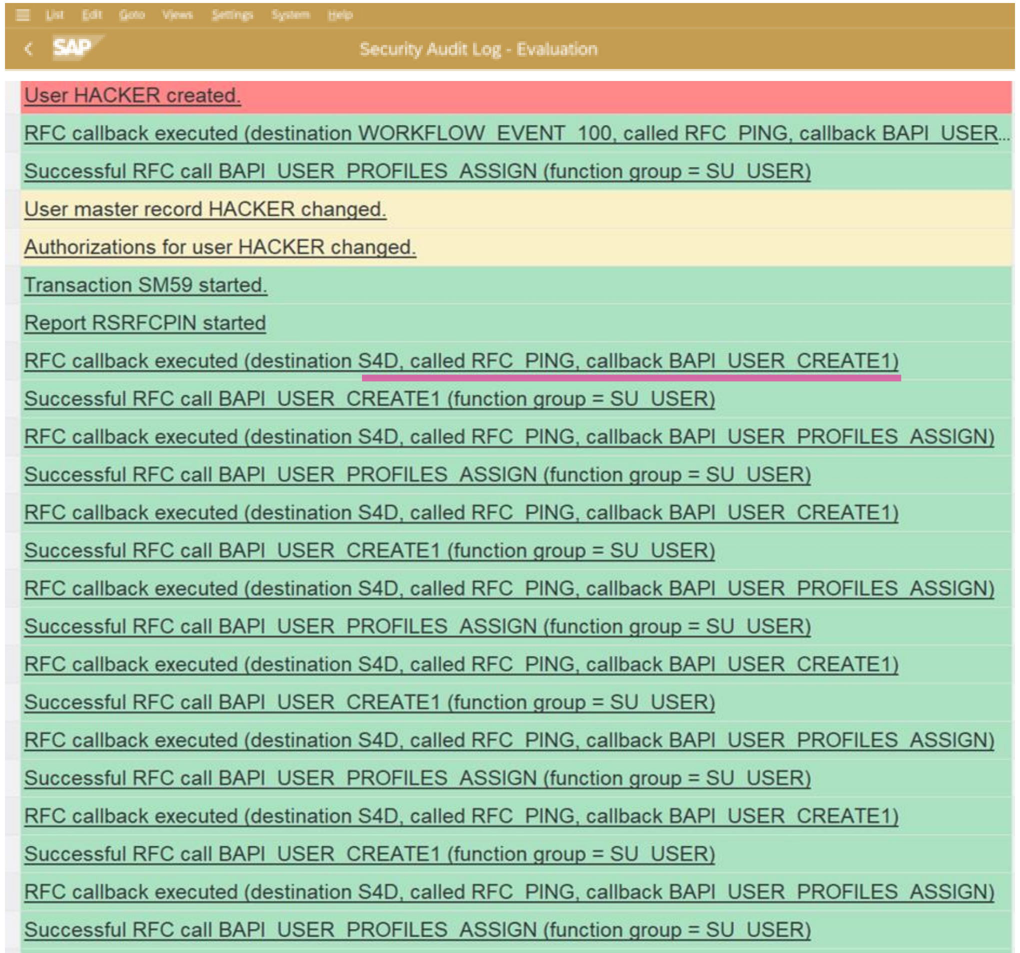
Was legitin

What changed on SRODRIGUES after creation?

Attack Example: Malicious RFC Callback

Using destination "BACK" when calling function modules in ABAP to link back the execution to the originally calling system

- Event DUI is triggered for each RFC Callback execution
- In Standard classified non-critical event
- Usable as lateral movement. (Hosting your own mini sap)
- Hard to judge with no SAP background



```
User HACKER created.
RFC callback executed (destination WORKFLOW_EVENT_100, called RFC_PING, callback BAPI_USER...
Successful RFC call BAPI_USER_PROFILES_ASSIGN (function group = SU_USER)
User master record HACKER changed.
Authorizations for user HACKER changed.
Transaction SM59 started.
Report RSRFCPIN started
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_CREATE1)
Successful RFC call BAPI_USER_CREATE1 (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_PROFILES_ASSIGN)
Successful RFC call BAPI_USER_PROFILES_ASSIGN (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_CREATE1)
Successful RFC call BAPI_USER_CREATE1 (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_PROFILES_ASSIGN)
Successful RFC call BAPI_USER_PROFILES_ASSIGN (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_CREATE1)
Successful RFC call BAPI_USER_CREATE1 (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_PROFILES_ASSIGN)
Successful RFC call BAPI_USER_PROFILES_ASSIGN (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_CREATE1)
Successful RFC call BAPI_USER_CREATE1 (function group = SU_USER)
RFC callback executed (destination S4D, called RFC_PING, callback BAPI_USER_PROFILES_ASSIGN)
Successful RFC call BAPI_USER_PROFILES_ASSIGN (function group = SU_USER)
```

SAP on Mitre ATT&CK

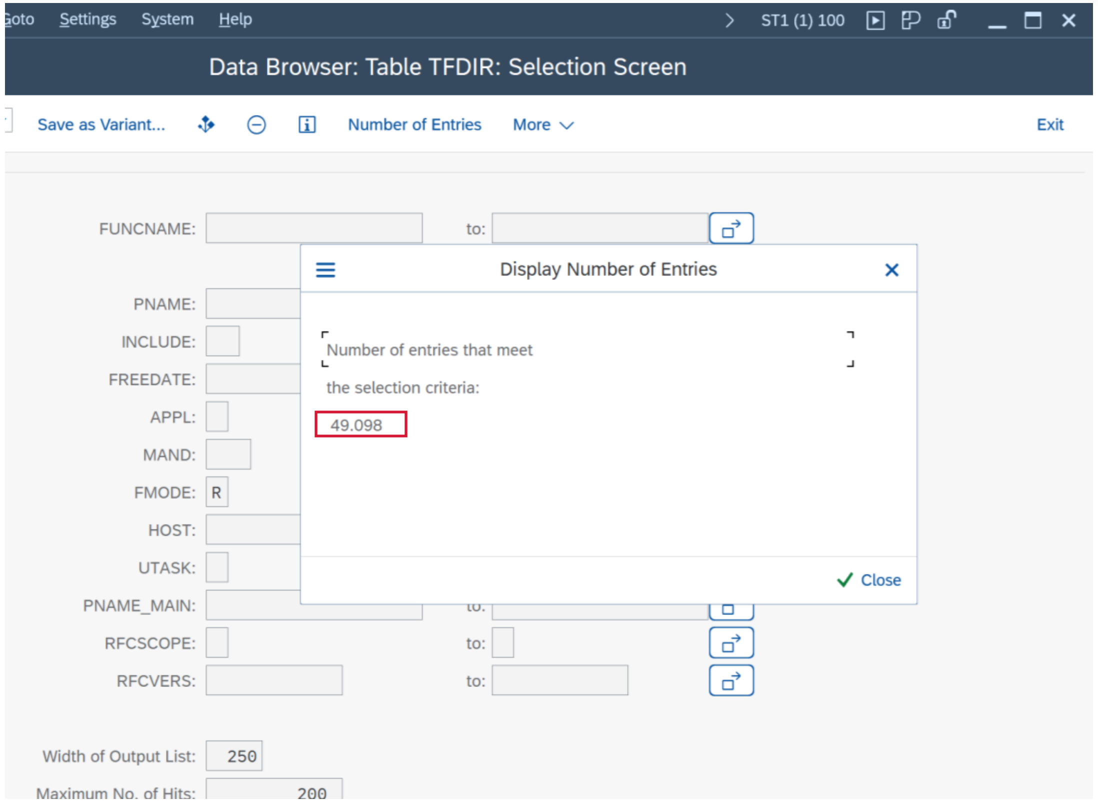
SAL Event ID AUK – Successful RFC call

Always:

- T1078 - Valid Accounts

Contextual:

- Almost any tactic depending on called function module
- E.g. T1021 - Remote Services



Data Browser: Table TFDIR: Selection Screen

FUNCNAME: to:
PNAME:
INCLUDE:
FREEDATE:
APPL:
MAND:
FMODE: R
HOST:
UTASK:
PNAME_MAIN: to:
RFCSCOPE: to:
RFCVERS: to:

Width of Output List: 250
Maximum No. of Hits: 200

Display Number of Entries

Number of entries that meet the selection criteria:

49.098

In the standard there are over 49.000 Remote procedure calls…

SOC Perspective on SAP with Mitre ATT&CK

SAL Event ID AUM

User *&B* Locked in Client *&A* After Erroneous Password Checks

Contextual:

- Credential Access:
  Brute Force T1110.001
  Password guessing
- Impact:
  Account Access Removal T1531

or PEBCAK ...

SAPanese 101

- Overcoming SAP Lingo
- Zero Trust / Assume breach
- Examples of cases given in Mitre DB
- Directly clear what would be worst case scenario

SOC Perspective on SAP with Mitre ATT&CK

SAL Event ID AUM

User *&B* Locked in Client *&A* After Erroneous Password Checks

Contextual:

- Credential Access:
  Brute Force T1110.001
  Password guessing
- Impact:
  Account Access Removal T1531

or PEBCAK ...

Keypoints on SAP and Mitre ATT&CK

- Multiple events can have the same ATT&CK ID‘s
- A single event can have multiple ATT&CK ID‘s
- Threat Modeling needs to be done cross department
- Mapping needs to be done manually… currently…
- No OOTB mapping available.. To be released soon!

Want to have your own SAP?

- Deployment of:
  - SAPRouter
  - SAP Cloud Connector
  - SAP System (S/4HANA)

Next Steps

Roadmap

Webpage

OpenSSF

Combine

Endorsement

Supporters

Supporters

OWASP®

pathlock

NO MONKEY

SECUREAUTH

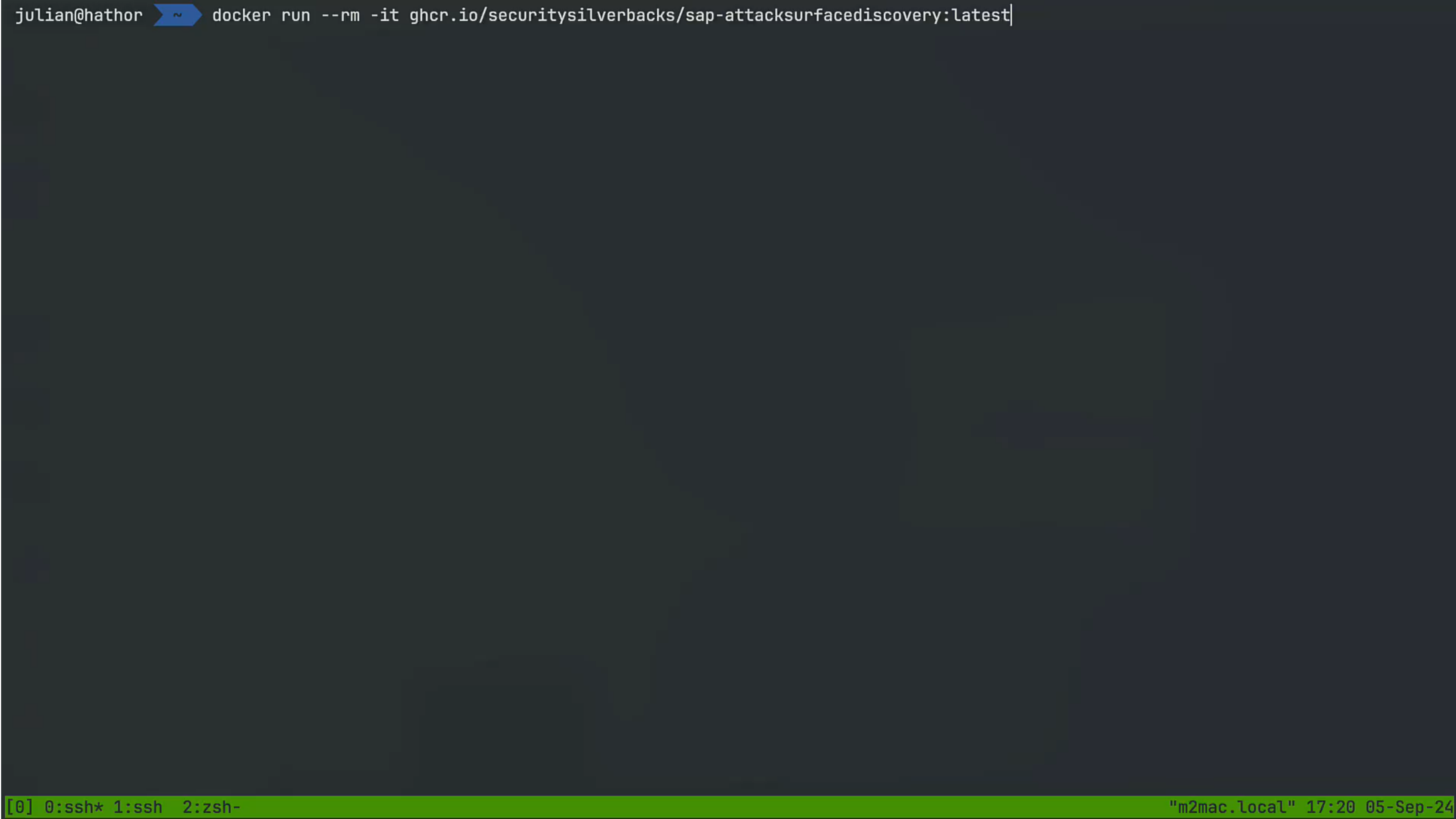
Security Bridge

more security. usd

Contributors

Q&A

Discord



```
julian@hathor  ~  docker run --rm -it ghcr.io/securitysilverbacks/sap-attacksurfacediscovery:latest
```

```
[0] 0:ssh* 1:ssh  2:zsh-                                                    "m2mac.local" 17:20 05-Sep-24
```