Identify, Exploit, & Defend SAP Environments

Showcasing the True Power of Open-Source

Core Business Application Security

Waseem Ajrab, NO MONKEY
Julian Petersohn, Fortinet

Speakers

Waseem Ajrab

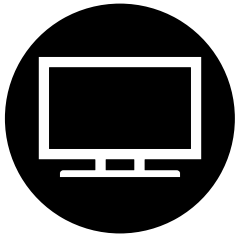
Julian Petersohn

Agenda

PROJECT GOALS

OWASP CBAS

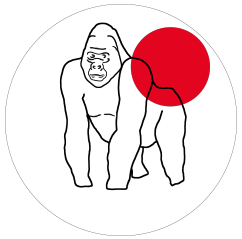
SAP SECURITY IN 2024



LIVE DEMO

SAP ATTACK SURFACE DISCOVERY

SAP SECURITY VERIFICATION STANDARD



OWASP®

SAP Complexity...

Is it a blessing or curse?!

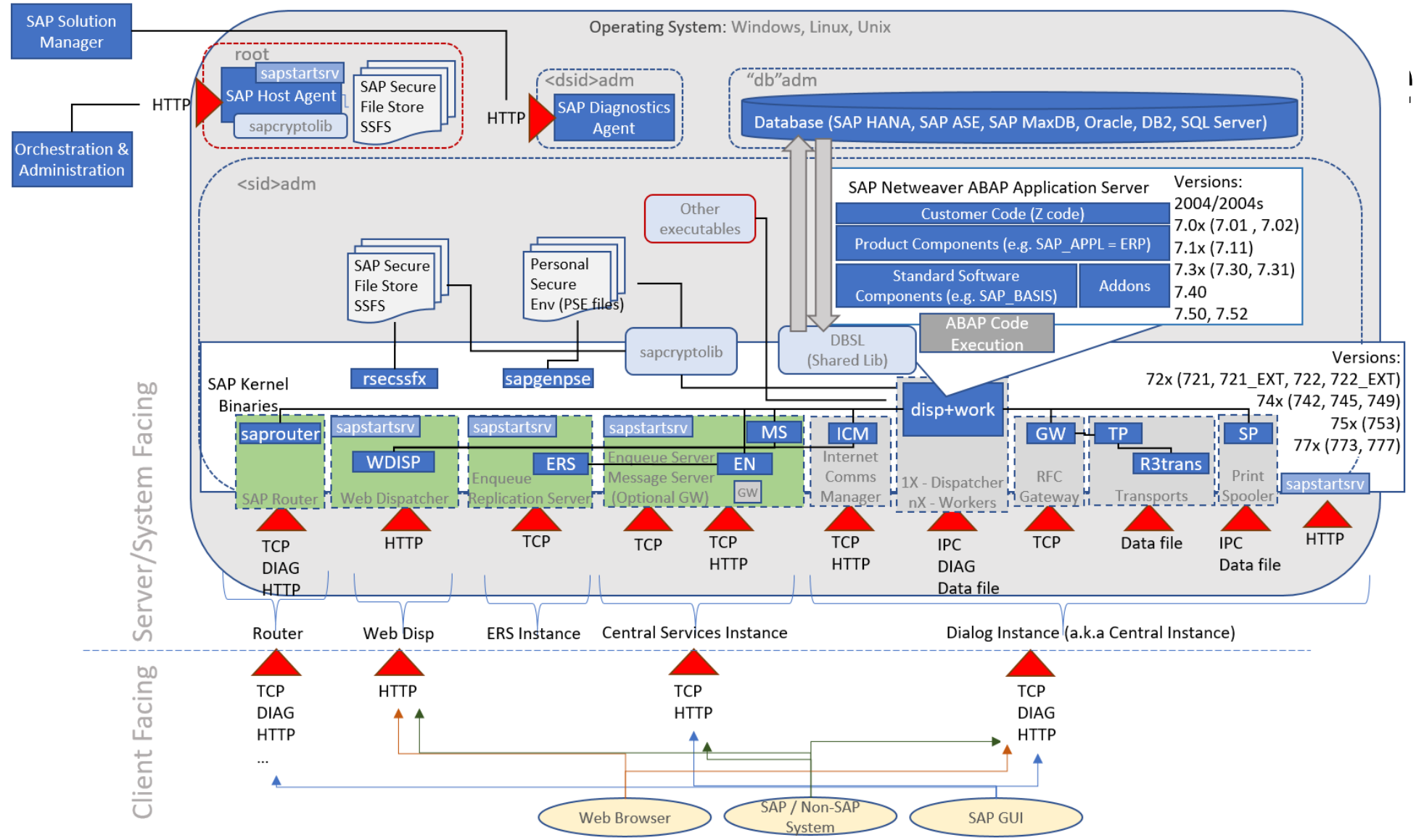
SAP Complexity – Application Level

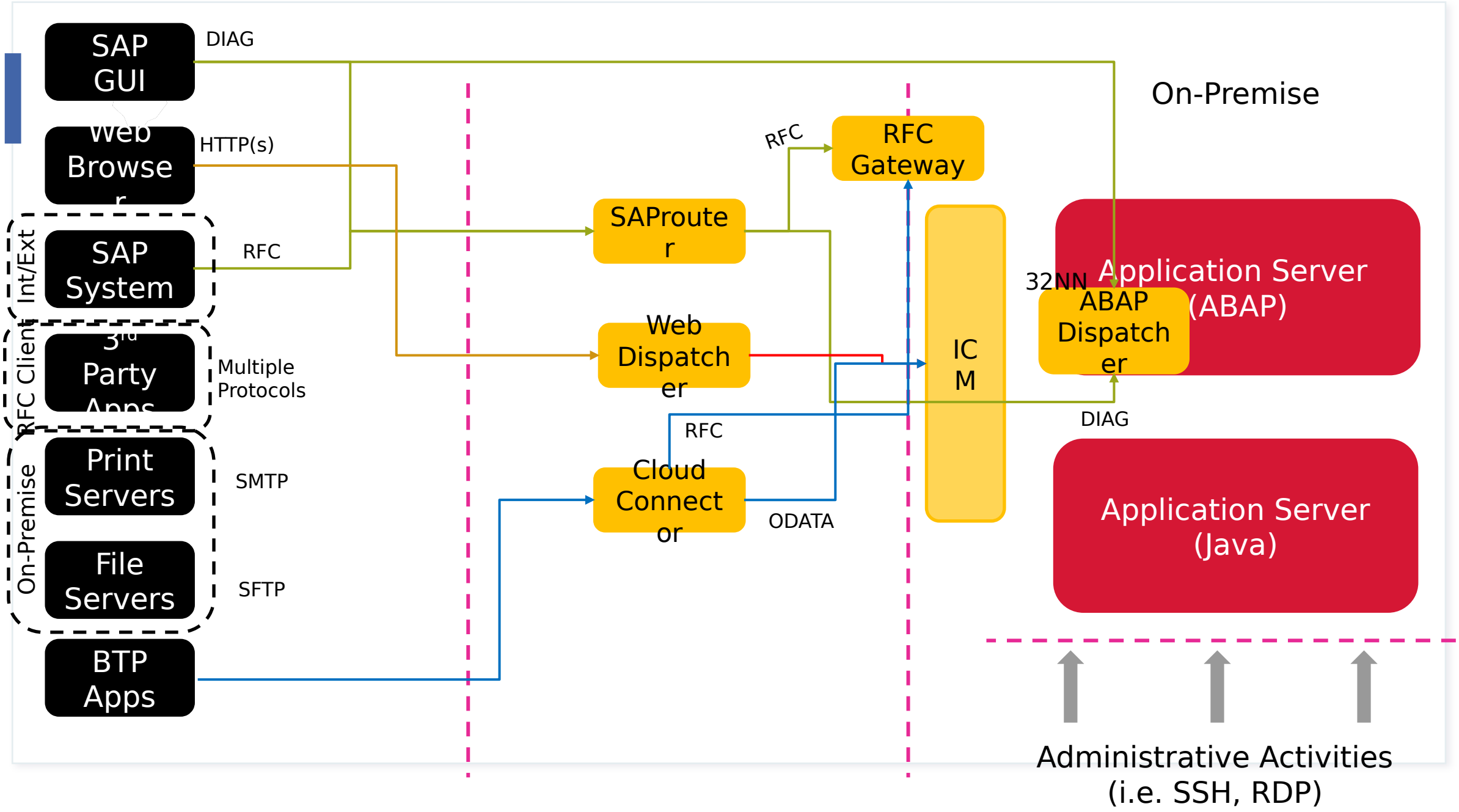
9,5	12	40	44	50	67	84

Windows 10

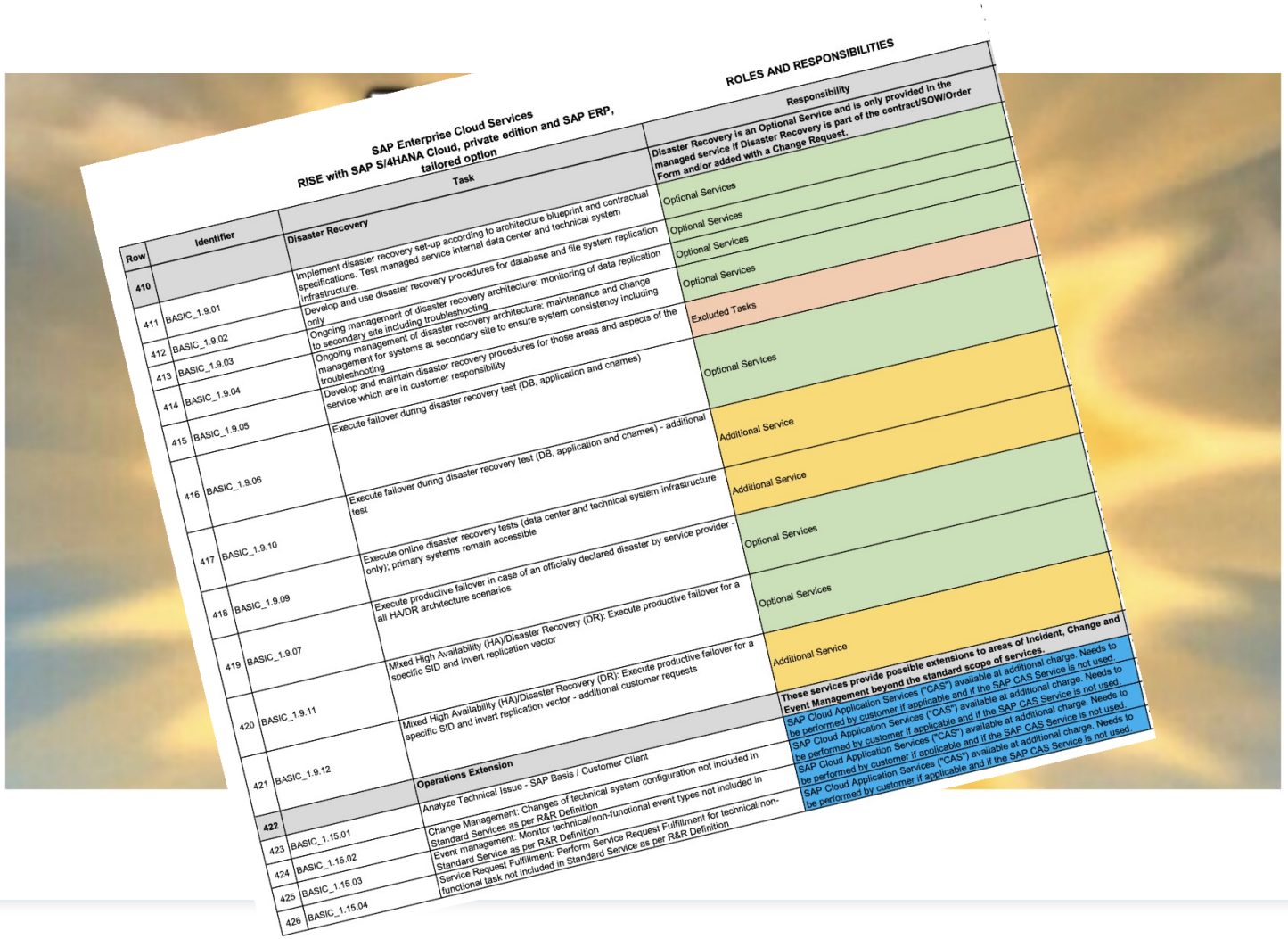
SAP Business Suite 319 Million Lines of Code (!)

SAP ERP 6.0 Entry Points



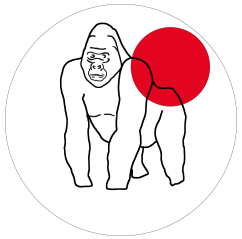

SAP GUI
DIAG
Web Browser
HTTP(s)
SAP System
RFC
Int/Ext RFC Client
3rd Party Apps
Multiple Protocols
Print Servers
SMTP
File Servers
SFTP
On-Premise
BTP Apps
SAProuter
RFC
RFC Gateway
Web Dispatcher
RFC
Cloud Connector
ODATA
ICM
On-Premise
32NN
ABAP Dispatcher
Application Server (ABAP)
DIAG
Application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

Row	Identifier	Task	ROLES AND RESPONSIBILITIES 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

OWASP®

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

WIZ

SAP Security Myths

OWASP®

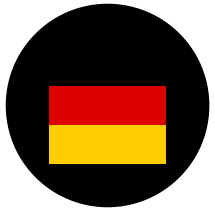
ZERO TRUST

IAM & AUTHORIZATION

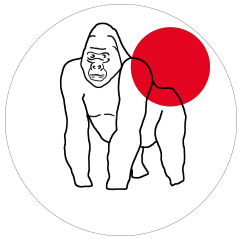
ENFORCING CONTROLS ONLY ON PRODUCTION

SAP BASIS TEAM TAKES CARE OF SECURITY

SAP SYSTEMS ARE ISOLATED AND NOT PUBLISHED



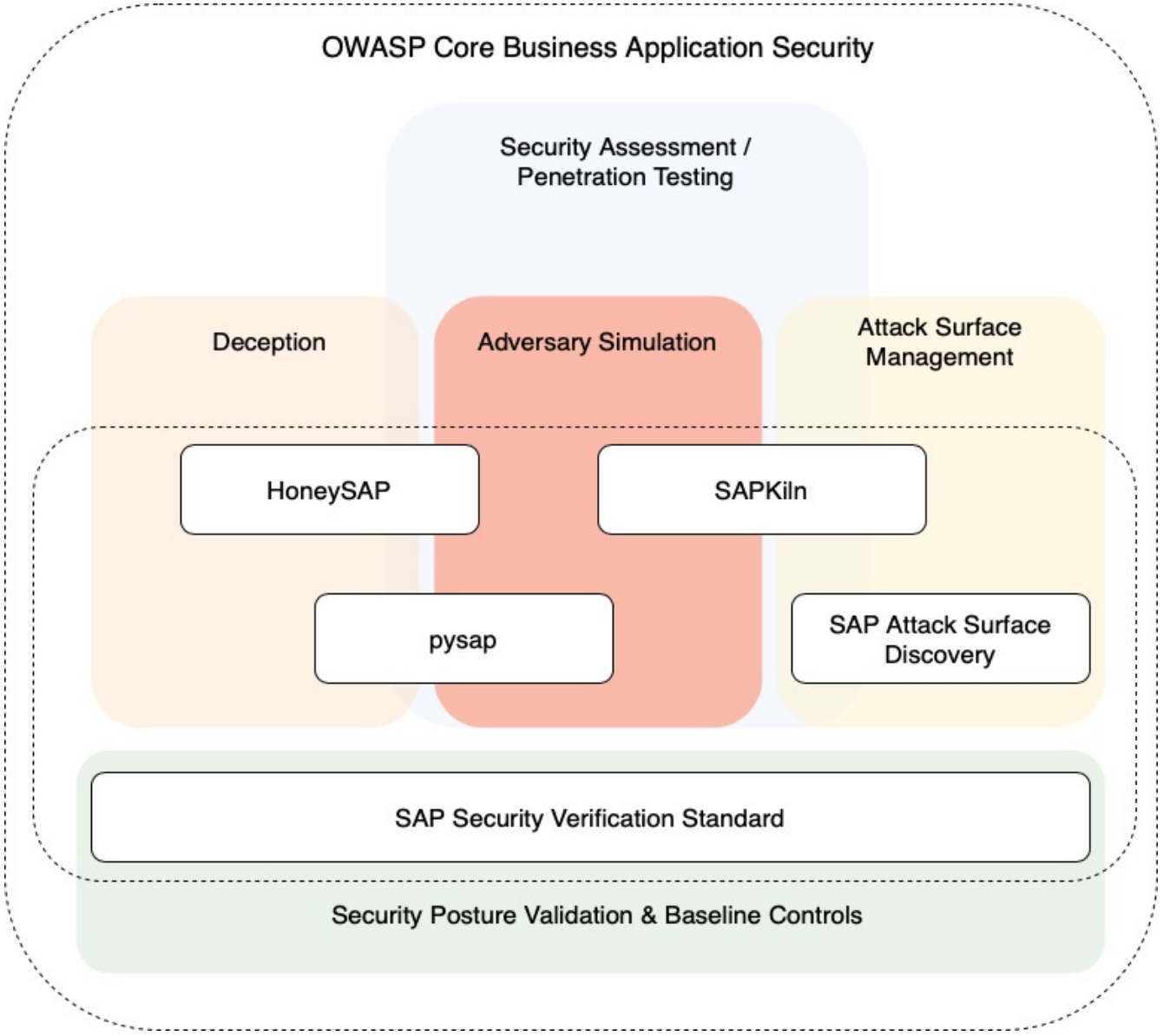
GERMAN MADE = SECURE BY DEFAULT



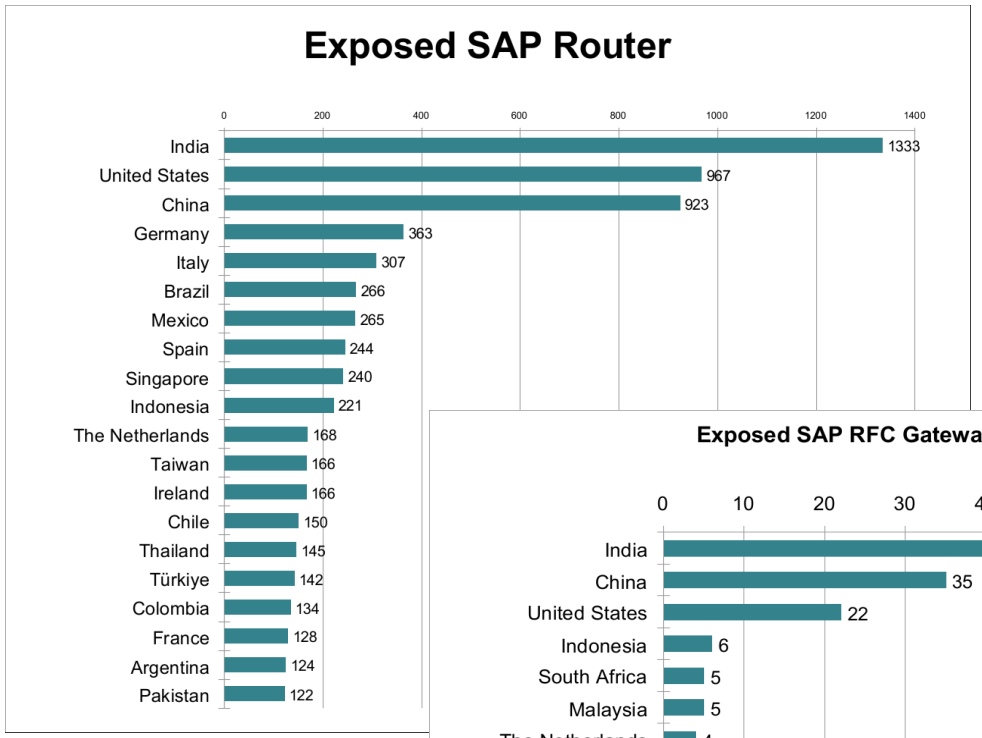
72% of beer production in the world depends on SAP!

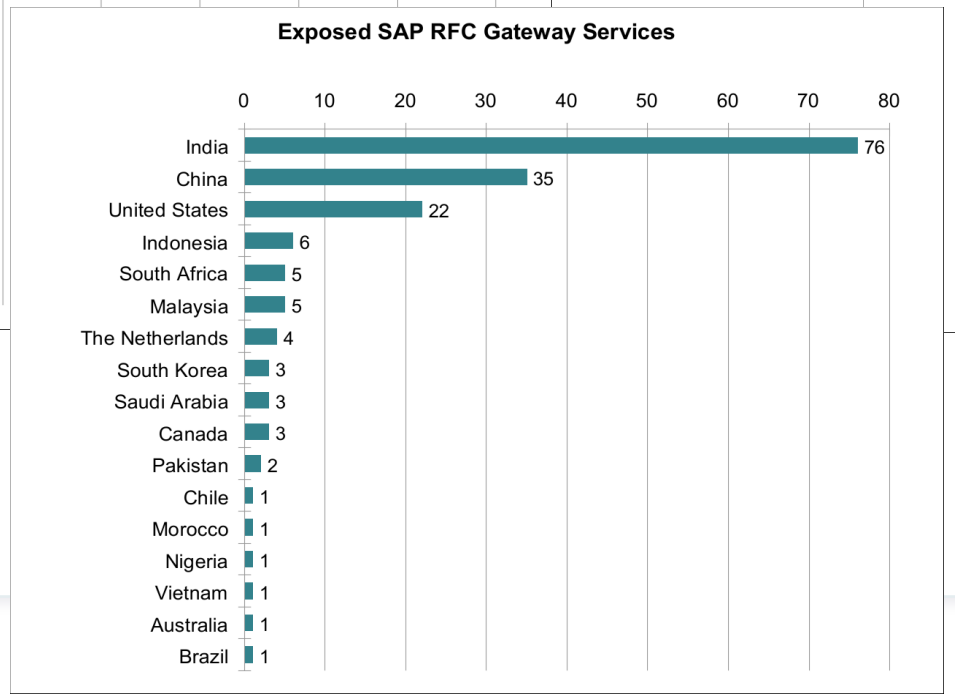
Project Goals

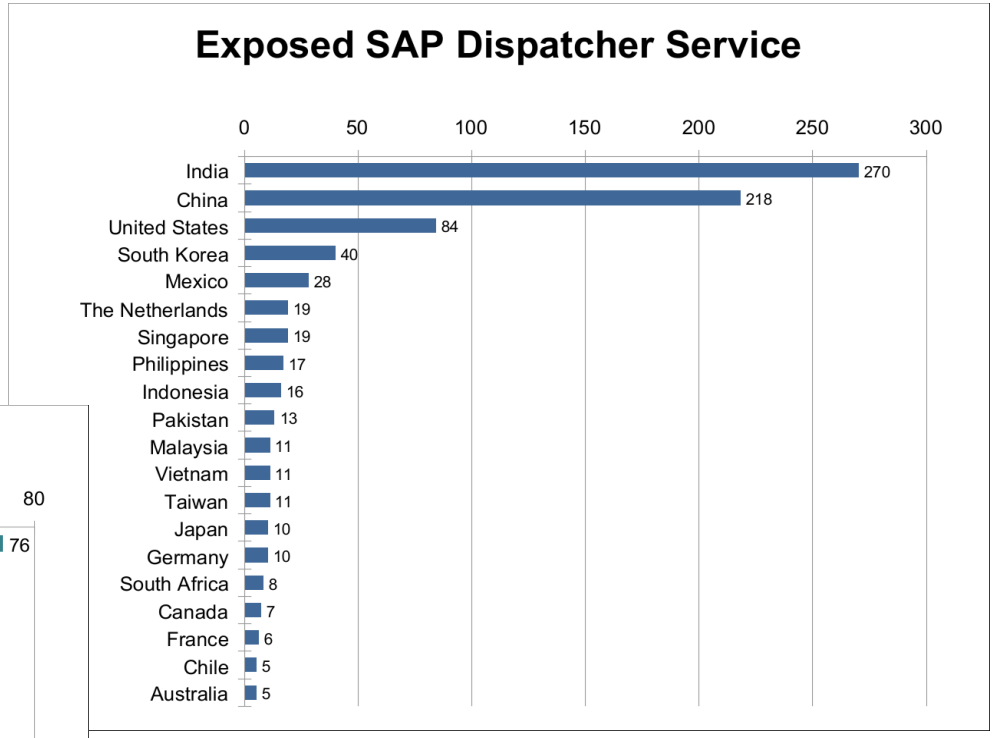
- Provide a security standard to secure SAP systems
- Provide the necessary tools to verify security measures
- Provide a single point of trusted security advisors
- Enabling regulators and auditors to assess enterprise business solutions


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

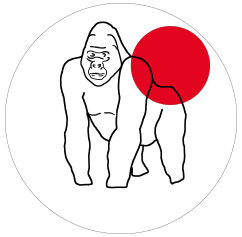
SAP Security in - a small period of - 2024





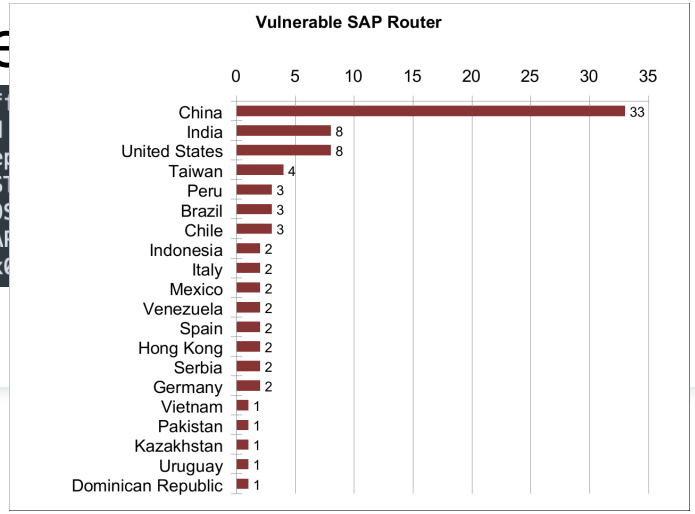


Attack Vector - SAPRouter



- 8793 public reachable SAPRouter worldwide
- Leaks version string within the error message
- Leaks the internal hostname of SAPRouter Server within the error message

```
\x00\x00\x01\x11NI_RTERR\x00(\x00\x00\xf
00\x00\xf9*ERR*\x001\x00connection timed
network interface)\x00749\x0040\x00D:/dep
/base/ni/nirout.cpp\x007966\x00RTPENDLIST
route received within 5s (CONNECTED)\x00S
00:54:08 2024\x00\x00\x00\x0064024\x00SAP
HRSAPSCM\x27\x00\x00\x00\x00\x00*ERR*\x0
```



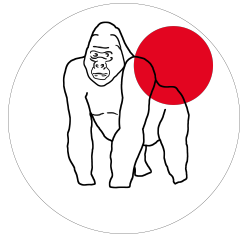
- 93 SAPRouter allows to dump Connection table
- Leaked internal services & IP addresses
- Provided a way for possible further attacks

```
[+]                :3299  -                :3299 - Connected to saprouter
[+]                :3299  -                :3299 - Sending ROUTER_ADM packet info request
[+]                :3299  -                :3299 - Got INFO response
[+]                :3299  - Working directory   : /usr/sap/saprouter
[+]                :3299  - Routtab             : ./saprouttab

[SAP] SAProuter Connection Table for
=====================================================

   Source     Destination     Service
   ------     -----------     -------
   10.1.      192.168.        sapdp00
   10.1.      192.168.        sapdp00
   10.1.      192.168.        sapdp00
```

Other Attack Vectors



SAP Dispatcher Information leak

```
[sap-dispatcher-detect:instance_details] [tcp] [info]                    :3200 ["DEV/SCORDN-DEV_DEV_00"]
[sap-dispatcher-detect:instance_details] [tcp] [info]                    3200 ["SMA/ROUTER_SMA_00"]
[sap-dispatcher-detect:instance_details] [tcp] [info]                    3200 ["HGJ/SAPGAMJA_HGJ_00"]
[sap-dispatcher-detect:instance_details] [tcp] [info]                    3200 ["IDS/linux-72wg_IDS_00"]
```

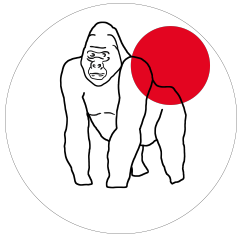
SAP Message Server Internal Configuration leak

```
[sap-message-server-internal-service-aclinfo-dump] [tcp] [high]                    :3900
[sap-message-server-check-monitor-status:Parameter] [tcp] [info]                   :3900 ["ms/monitor =0"]
[sap-message-server-check-admin-port:Parameter] [tcp] [info]                       :3900 ["ms/admin_port =0"]
```

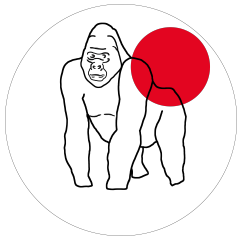
Usage of Default Credentials

```
[*] Testing None:3200
[*] Not discovering clients, using 000,001,800 or client supplied in credentials file
[+] Valid credentials found:    Client: 000     Username: SAP*  Password: PASS  Status:
[+] Valid credentials found:    Client: 800     Username: SAP*  Password: PASS  Status:
[+] Valid credentials found:    Client: 000     Username: DDIC  Password: 19920706      Status:
```

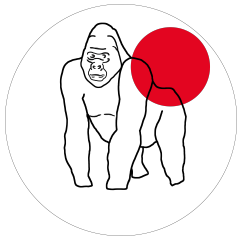
Attack Flow



Find open ports → Enumerate services → Scan & test for default credentials → validate access & check permissions → Compromise system

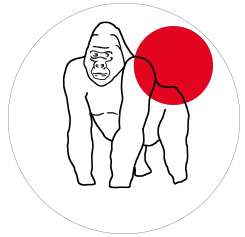


Live Demo



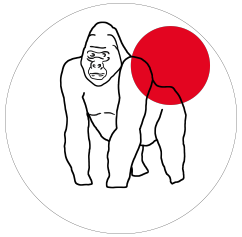
SAP Attack Surface Discovery

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?

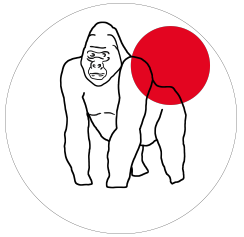


- Containerized environment
- Nuclei Templates
- Wiki section per service
- Collaboration with hunter.how
- Inclusion of Shodan queries

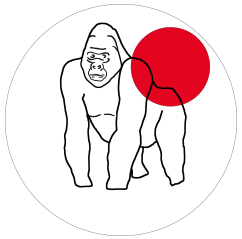
Services added so far:

- 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)

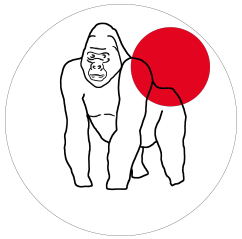
Roadmap



- 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



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

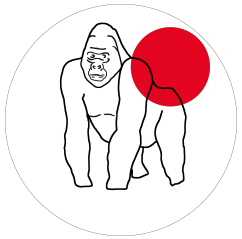
Description

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

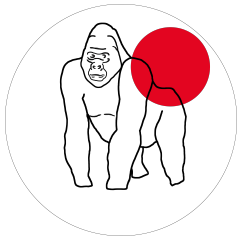
The below standard users, found in ABAP systems, are required to be managed and securely configured: (The Verification of Control section will help organizations have the basic requirements to secure these users)

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.

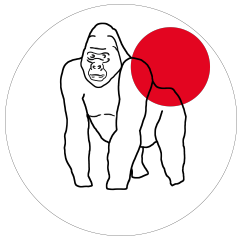
Implementation

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.

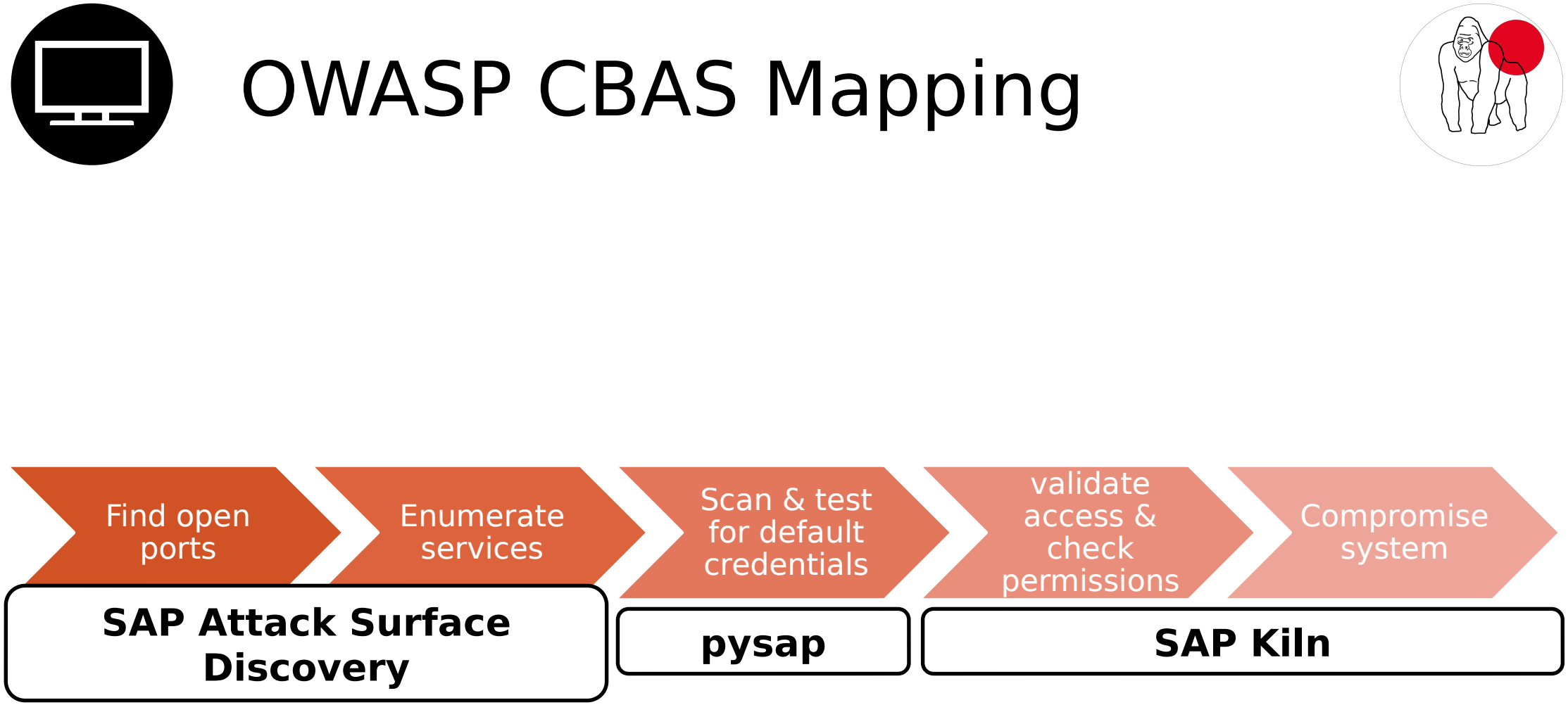


Pysap

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.

OWASP CBAS Mapping



Want to have your own SAP?

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

Q&A

Discord