SAP Secure Operations Map

SAP CoE Security Services
October 2017
The SAP Secure Operations Map

• is a Reference Model
to structure the broad area of security for content, discussions and as a basis for a 360° view on security – i.e. you can’t “order” a block, but you can allocate discussions, needs and solutions to specific security areas

• focuses on the Operational Aspects of security
– i.e. on the tasks and considerations which a customer or service provider has to take into account to maintain and operate their systems and landscapes in a secure manner.

• is further interpreted in the concrete Context of SAP Systems, although the model also could be applied to non-SAP realms.
The “Security Compliance” layer focuses on the governance and regulations around the SAP systems, to which the SAP systems have to adhere themselves – e.g. general or IT-specific Security Policies, Audit requirements or Emergency Plans.

The three middle layers of the Secure Operations Map directly apply to the operation of SAP systems themselves. The further discussion of the Secure Operations Map will focus on these three layers.

The “Infrastructure Security” layer focuses on SAP-specific requirements towards the non-SAP technical environment – e.g. network, operating systems, non-SAP databases, clients.
Security Maintenance of SAP Code

- SAP is continuously doing a high investment to develop and deliver secure code to its customers. Nevertheless, security updates of already delivered code are required regularly due to new attacks and new vulnerabilities.
- Customers need to establish a corresponding Security Maintenance process to ensure a regular and suitable consumption of these security updates – code corrections as well as configuration recommendations.

Custom Code Security

- The first step in Custom Code Security is proper Custom Code Management: Unnecessary custom code should be removed, required custom code should be maintained in a proper Custom Code Lifecycle Management.
- Custom Code Lifecycle Management should cover the whole lifecycle from secure architecture & design via secure development – including but not restricted to the use of code security scanners – up to secure deployment, security maintenance and finally custom code retirement.
Secure Configuration

- Secure Configuration foremost deals with suitable secure settings of relevant system parameters and other configuration settings. It also includes activation of security features and functionalities, which may be switched off initially for backward compatibility and migration purposes.

Communication Security

- This part deals with the security of communication connections – from connection lifecycle management via proper management of communication users and authorizations up to encryption of communication lines and the corresponding cryptographic key management.

Data Security

- Data Security deals with the security of data at rest – change and read access control and logging, purpose-driven encryption of sensitive or all data and additional protection mechanisms like data masking.
Users and Authorizations

- This is often the most well-known area of operational security, since operation of a system does not work without. It includes the lifecycle management of users accounts in systems and landscapes, proper assignment, maintenance and revocation of authorizations and control of compliance and segregation of duties (SoD).

Authentication and Single Sign-On

- Authentication deals with the verification of the true identity of a claimed user. It may be as simple as a password, may include multi-factor mechanisms and may also deal with trusted system connections in which one systems relies on the correct authentication by another system.
- Single Sign-On establishes an infrastructure, in which a user authenticates himself once in a landscape to then get access to several systems without the need for repeated additional authentication.
Support Security

- The topic area of “Support Security” does not only deal with external support – as e.g. provided by SAP – but also includes internal support teams. Whoever is providing support often needs extended access and authorizations to be able to help. Such extended rights should be tightly controlled and properly maintained. Only such rights should be permanently assigned which are required on a regular basis. Others should be only assigned when needed, e.g. via an emergency process or user. Support activities should also be monitored and controlled to ensure security by limitation to the real need.

Security Review and Monitoring

- With today’s powerful attacks and complex landscapes, proactive security is absolutely required but not sufficient. It needs to be enhanced by reactive security mechanisms, which are able to identify security weaknesses and breaches and thus allow to properly counter them. This includes review and validation activities as well as life monitoring of system operations and triggering appropriate countermeasures in case of an attack or some suspicious system behaviour.
How to use the Secure Operations Map

Be aware:

“Security” is not a property which you have or don’t have. It is a risk measure, where you can have a higher or lower level of Security.

Maximum Security is often not what you want, since this requires high effort and may limit functionality. You require adequate security:

- Baseline measures / Security Best Practices should always be applied.
- For systems with security needs beyond such baseline measures, a risk analysis is required to derive corresponding suitable additional security measures.

“Security” often is invisible. The fact, that you don’t notice security weaknesses or successful attacks, does not mean that there are not any.

“Security” does not only protect against malicious attacks but also against unintended failures.
How to use the Secure Operations Map

Therefore use the Secure Operations Map as a structure to informally identify areas and topics which are most important to address.

Do not try to cover at once every area in all details.

Revisit security on a regular (e.g. yearly) basis. New functionality and new technologies require new security measures. New attack patterns arise and need to be countered.
The 16 Secure Operation Tracks cover the following topics:

**Security Governance:** Adopt security policies for your SAP landscape, create and implement an SAP Security Baseline

**Audit:** Ensure and verify the compliance of a company’s IT infrastructure and operation with internal and external guidelines

**Cloud Security:** Ensure secure operation in cloud and outsourcing scenarios

**Emergency Concept:** Prepare for and react to emergency situations

**Users and Authorizations:** Manage IT users and authorizations including special users like administrators

**Authentication and Single Sign-On:** Authenticate users properly – but only as often as really required

**Support Security:** Resolve software incidents in a secure manner

**Security Review and Monitoring:** Review and monitor the security of your SAP systems on a regular basis

**Secure Configuration:** Establish and maintain a secure configuration of standard and custom business applications

**Communication Security:** Utilize communication security measures available in your SAP software

**Data Security:** Secure critical data beyond pure authorization protection

**Security Maintenance of SAP Code:** Establish an effective process to maintain the security of SAP delivered code

**Custom Code Security:** Develop secure custom code and maintain the security of it

**Network Security:** Ensure a secure network environment covering SAP requirements

**Operating System and Database Security:** Cover SAP requirements towards the OS and DB level

**Frontend Security:** Establish proper security on the frontend including workstations and mobile devices
Thank You!

Contact information:

SAP CoE Security Services
securitycheck@sap.com