IT Security

Chapter 6: Secure Software Engineering

Part 1

- Process model
- Analysis of safety requirements
- Security architecture and design
- Security analysis tools

Prof. Dr. Reiner Hüttl, TH Rosenheim, © 2023, 15.03.2023

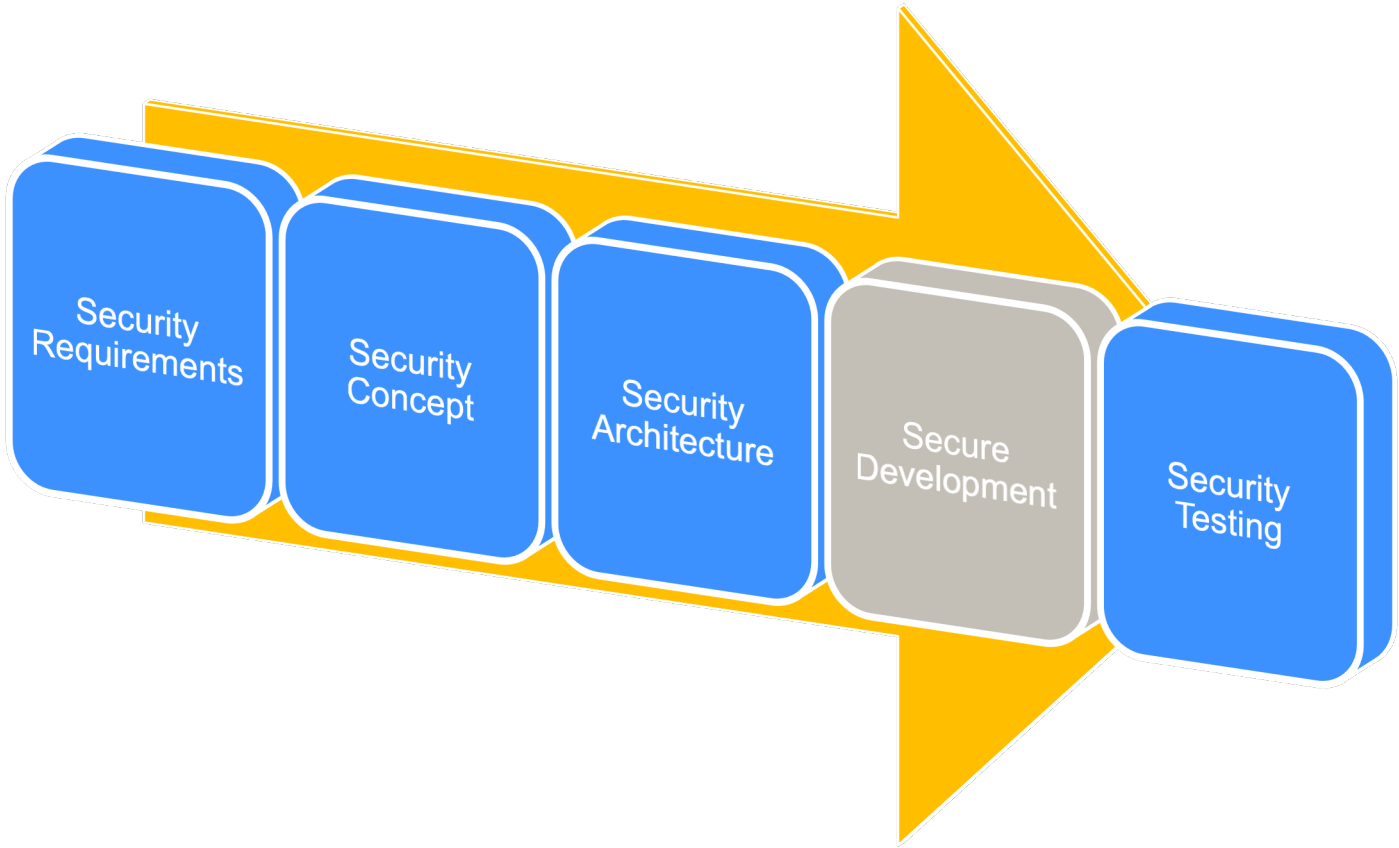
What do we want to learn?

- How do we get security into the software engineering process?
- What should we consider regarding security before implementation?
- What are the design principles for security?
- How can I verify security in my IT-System?

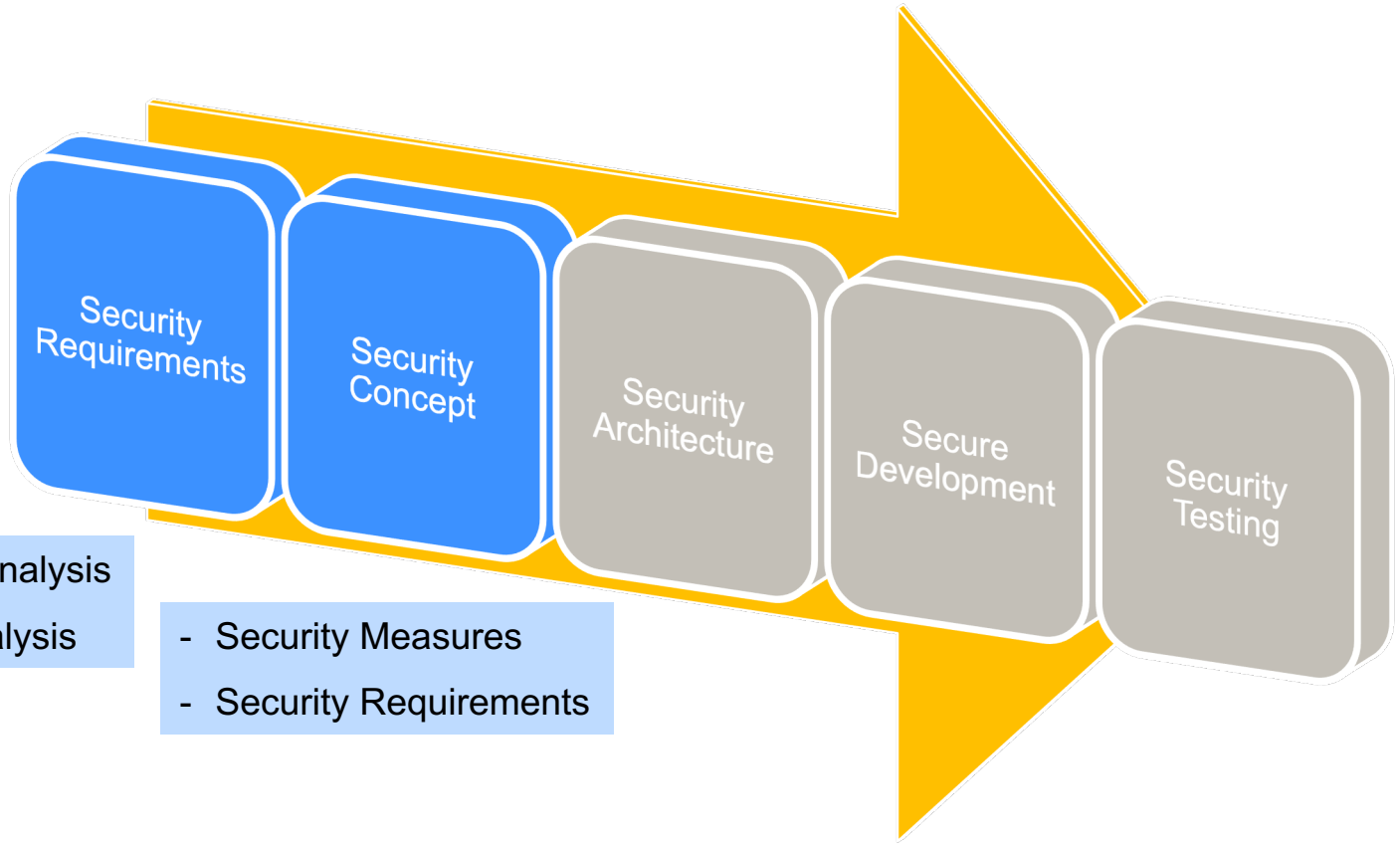
Why Secure Software Engineering?

- Insecure software can cause nasty surprises

The phases of Secure Software Engineering



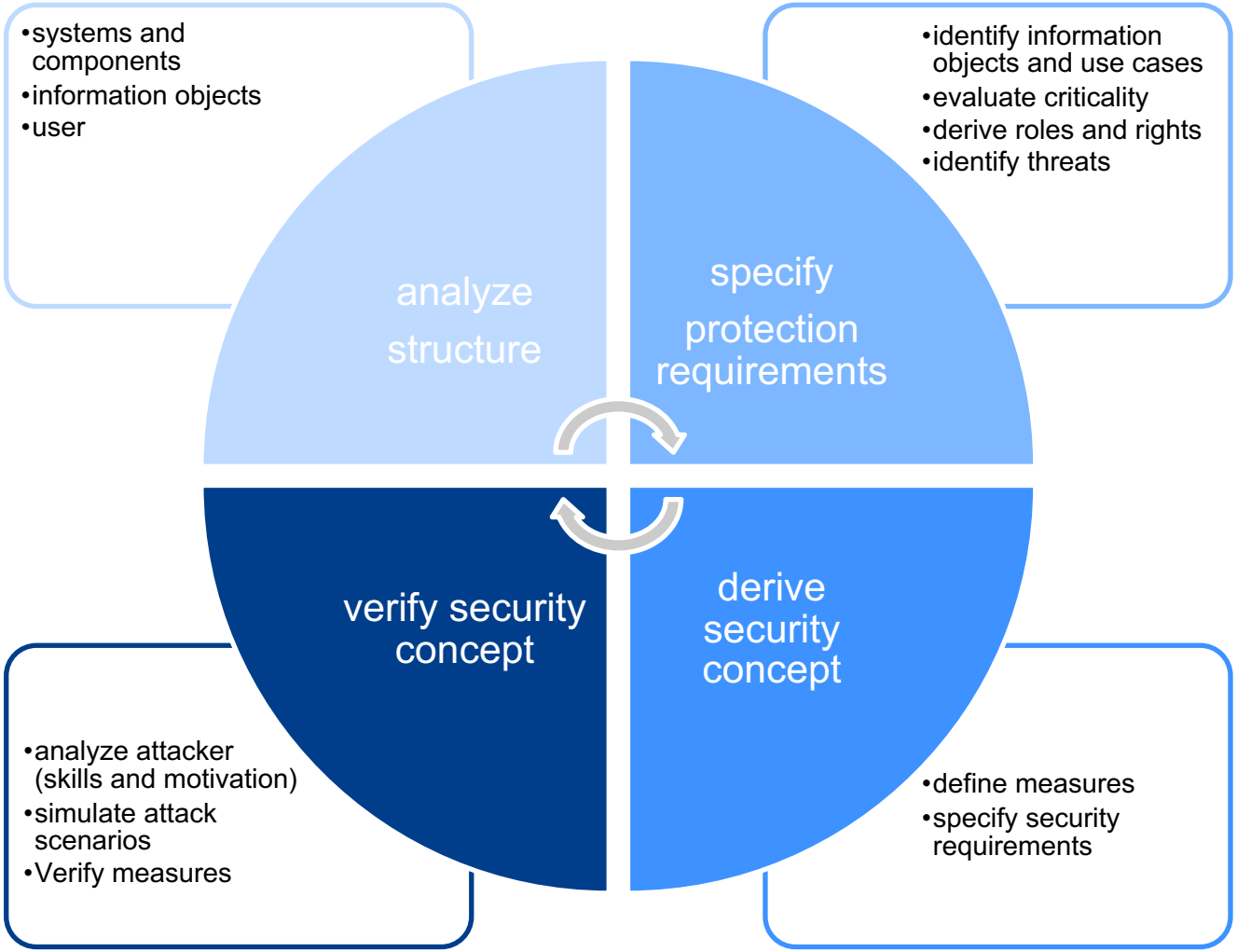
The requirements and concept phase



- Threat Analysis
- Risk Analysis

- Security Measures
- Security Requirements

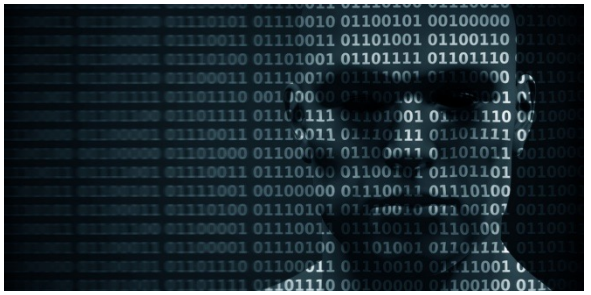
A process model for security analysis



Step 2 in the process model: specify the protection requirements

- Identify critical information objects
  - Evaluation regarding security objectives (CIA)
  - What is the damage if security objectives are violated?
- Evaluate the protection requirements of the use cases
  - Which use cases cause high damage if security objectives are violated?
  - Also consider technical use cases (e.g., certificate management, system administration, authorization assignment).
- Assign roles and rights in the system
  - Which users/roles are there?
  - Who is allowed to do what?
  - Establish access control principles ("need to know", "segregation of duties", ...)
- Identify and analyze threats
  - Threat Modeling
  - Risk analysis

A modell for Threat Analysis



Microsoft Threat Model: STRIDE

- **S**poofing
  - Users should not be able to become any other user or assume the attributes of another user
- **T**ampering
  - Data tampering involves the malicious modification of persistent data and data over networks.
- **R**epudiation
  - Users may dispute transactions if there is insufficient auditing or recordkeeping of their activity

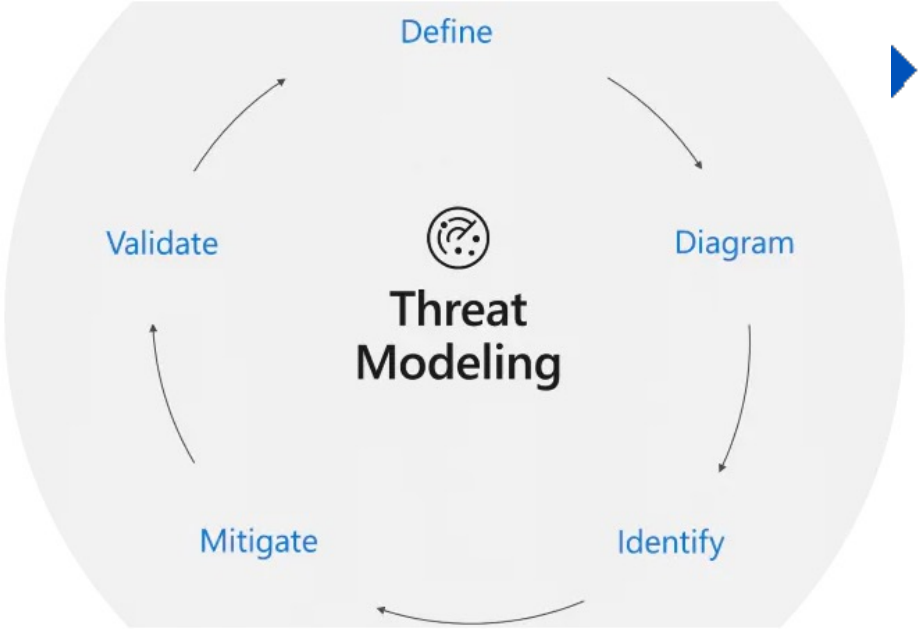
https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

STRIDE

Microsoft Threat Model: STRIDE

- **I**nformation Disclosure
  - The exposure of information to individuals who are not supposed to have access to it
- **D**enial of Service
  - Deny service to valid users—for example, by making a Web server temporarily unavailable or unusable
  - .
- **E**levation of Privilege
  - An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system

Microsoft Threat Modeling



- There are five major threat modelling steps
  - defining security requirements
  - creating an application diagram
  - identifying threats
  - mitigating threats
  - validating that threats have been mitigated

Quelle: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Microsoft Thread Modeling Tool https://aka.ms/threatmodelingtool

- Alternative approaches to threat analysis
  - Misuse cases
  - Attack trees
  - Threat catalogs

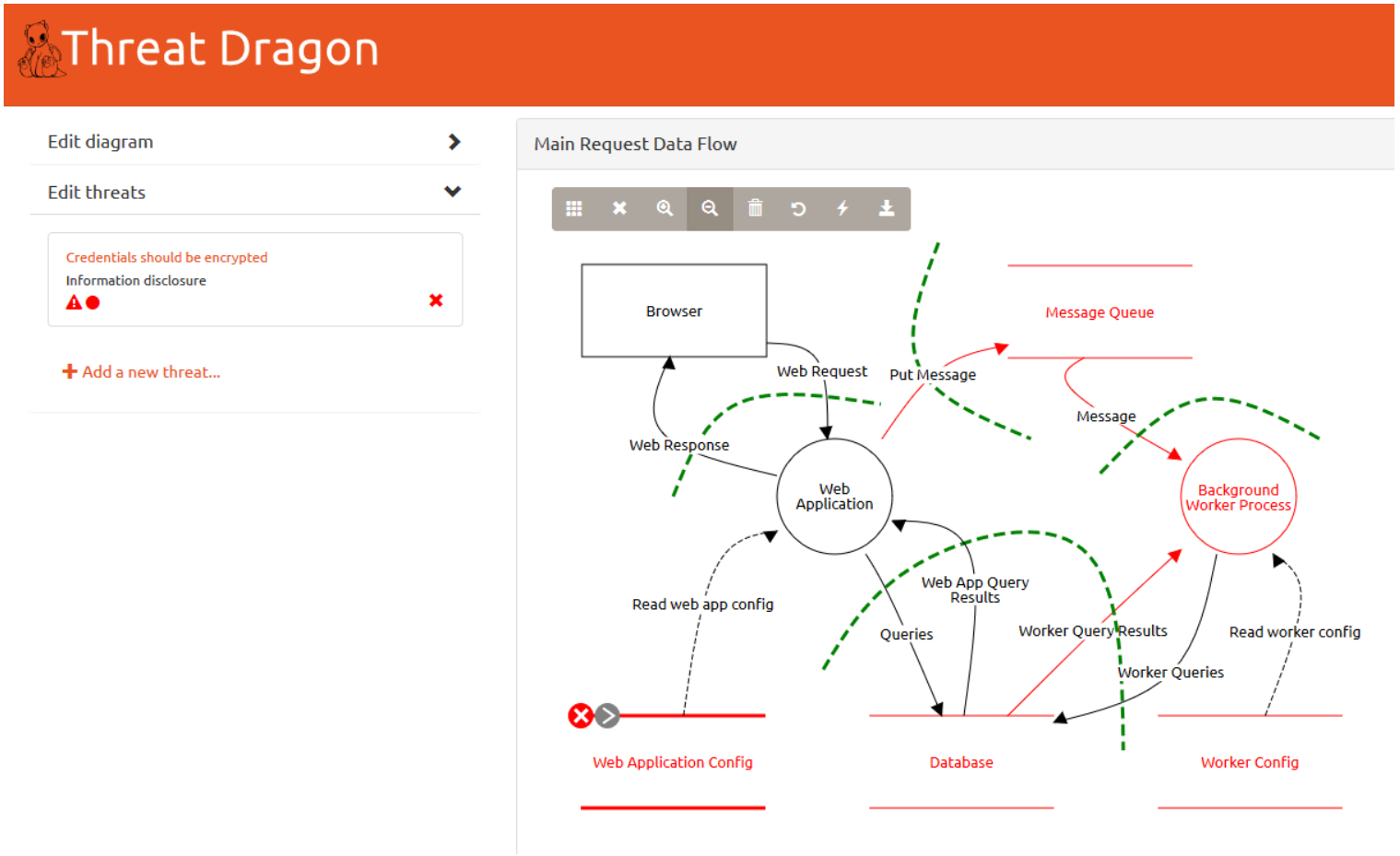
Weitere Informationen in:
Matthias Rohr: Sicherheit von Webanwendungen in der Praxis, Springer Vieweg, 2018 **(E-Book)**

Threat Modeling Process

https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

- Decompose and model the system
  - Create an application diagram (processes, data store, actors)
  - Describe data flow (data in transit and at rest)
  - Define trust boundaries
- Identify Threats
  - Define all possible threats
  - Identify attack vectors, attack trees and misuse cases
  - Map threat agents to application entry points
  - Define the impact and probability for each threat
    → **Risk Analysis**
- Determine Countermeasures and mitigation
  - Identify risk owner (responsible for mitigation)
  - Build risk treatment strategy (Reduce, Transfer, Avoid, Accept)

Sample Model from modeling tool OWASP Threat Dragon



https://owasp.org/www-project-threat-dragon/

Example for Threat Modeling with STRIDE: Identify threats and assign type and mitigations

Threat	Type	Mitigation
Unauthorized request to DB	I	All queries to be authenticated
DB Credential Theft	I	Use FW to restrict access to DB to only background Worker IP
Message Tampering in Message queue	T	Sign all messages
Fake massages in queue	S	Implement authentication on queue
Generate malicious messages that Background Worker cannot process	D	Validate content of messages before processing, reject messages with invalid content, log the rejection, do not log the malicious content
Brute forcing of Web Application Login	E	Slowdown login attempt after unsuccessful login, 2FA for admin accounts
Sniffing of Web requests	I	Https Encryption of all requests
SQL injection	T	Input validation
Undocumented change of Web App Config	R	Auditing all changes in Web App Config, access control to Web App Config

Risik Analysis

- A comprehensive risk/threat analysis is costly and time-consuming
  - often the customer/client is not ready for it
  - → Perform a pragmatic risk analysis
- Focus on the most important risks
- Focus on data criticality and interfaces
- Risks must be assessed by the responsible parties (ISO, DPO, product owner, management)
- Establish transparency about the assessment of risks
  - Review by ISO/DPO

Risk analysis for Logging

Logstash **Kibana**

- We consider logging in a cloud application as an example
- Security Goals

  - The root cause of incidents or faulty platform or application behavior can be adequately analyzed and identified.
  - Required log data and analysis tools are available and correspond to the actual state of the system at the relevant time.
  - The technical logs are secured from unauthorized access and manipulation.

Risks at Logging

- **R-1: Missing log data.** An incident cannot be sufficiently analyzed because relevant log information for the required period of time has not been collected, e.g. due to a misconfiguration/failure of the log stack or according infrastructure components.

Availability

- **R-2: Loss of log data.** Log information gets lost, e.g. due to a failure of the log storage.

Integrity

- **R-3: Manipulation of logs.** The root cause of an incident can be hidden or obscured by modification or deletion of log data.

Availability

- **R-4: No access to log data.** Relevant log data cannot be viewed when required due to blocked access, e.g. missing credentials

Confidentiality

- **R-5: Disclosure of sensitive log information.** Information written to log files can give valuable guidance to an attacker or expose sensitive user data

Compliance

- **R-6: Violation of deletion obligation.** To store log files longer than the allowed retention period violates compliance (e.g. GDPR)

Risk-Control-Matrix for Logging

System Component	Risk	Risk name	Mitigating measures
Logging	R-1	Missing log data	- all logs are collected and stored in a central managed log stack - log configuration is maintained by DevOps experts - regular review of all critical assets for their correctness and currency - mechanism to ensure that all required logs are captured (e.g. via documented search in logging system, configuration rule/policy)
Logging	R-2	Loss of log data	- backup of log data by AWS - storage of log data provided by AWS in a managed ELK stack - retention of 30 days - independent monitoring of logging software with alerting in case of failure
Logging	R-3	Manipulation of logs	- log data secured by AWS - access control via IAM - measures for integrity - audit the access to log data
Logging	R-4	No access to log data	- availability is provided by AWS
Logging	R-5	Disclosure of sensitive log information	- isolation of application log data (separate storage and access control for different applications/tenants) - role-based access control to logs - encryption of data at rest, decryption key only available to application owner - transport of log data is secured with minimum TLS 1.2
Logging	R-6	Violation of deletion obligation	- complete deletion of log data immediately after end of retention period - there are no local copies / snapshots of log data (enforced by policy) - deletion process according to GDPR and security needs

The result of the security analysis is a Security Concept