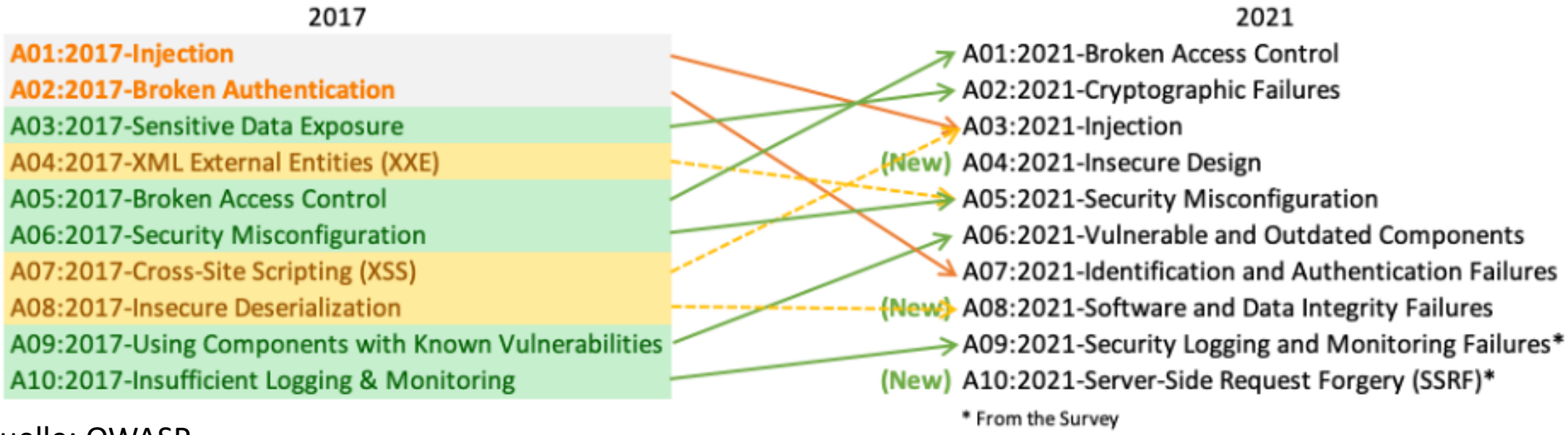
Trends in der Softwaresicherheit

– Unsicheres Design und „Denkfehler“ lösen Sicherheitslücken technischer Natur als wesentlichen Risikofaktor ab.



Quelle: OWASP

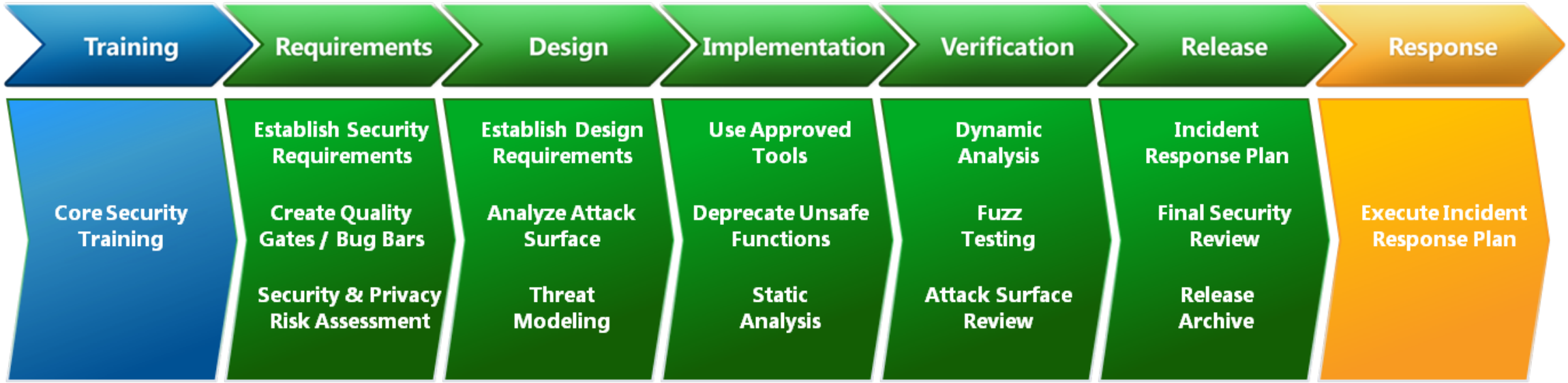
Trends in der Softwaresicherheit (2)

- Der Einsatz von Low-Code/No-Code-Plattformen verstärkt diesen Effekt weiter.
- Dazu bringen sie neue einzigartige Risiken mit.
- Was können wir tun?

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

Quelle: OWASP

Was können wir tun?



- "Shift Left": neben rein technischen sind vor allem organisationelle Maßnahmen angezeigt.
- Schulung des Personals im Umgang mit der Plattform,
- Sensibilisierung für häufige Bedrohungen, Best Practices.

Was können wir tun? (2)

- Rollen- und Berechtigungskonzepte sind ein wesentlicher Aspekt in der LCNC-Sicherheit.
  - Bürger,
  - Antragstellende,
  - Behörden,
  - Fachverfahren,
  - Administratives Personal

- Diese Konzepte müssen selten einzigartig sein und so können wir starke Vorschläge bzw. Vorgaben machen.

Was können wir tun (3)

- Nudging kann effektiver als Zwang sein ☺

- In der Entwicklungsumgebung selbst über Bedrohungen und Risiken einzelner Bausteine oder Verbindungen aufklären.
- Für häufige unsichere Konstruktionen Gegenvorschläge anbieten, die mit einem Klick eingebaut sind.
- “Summary” über Sicherheitszustand, z.B. Anzahl privilegierter Rollen pro Baustein, mit Historie.