
SBA
Research

SBA Research
Professional Services

Security Governance

- Security Governance Lagebild
- ISMS / ISO 27001
- Compliance (NIS-2, CRA, DORA, etc.)
- Risikomanagement & Business-Impact
- Audit & Beratung

Cyber Defense

- Cyber Security Lagebild
- Penetrationstests (Infrastruktur, Cloud, Netzwerk)
- Red/Blue/Purple Teaming
- Social Engineering & Phishing
- SWIFT CSP Audit

Security Schulungen

- Security Awareness
- Hacking & Defense (Web, Windows, IoT)
- Secure Coding & Application Security
- Cloud & Cloud-Native Security
- Zertifizierungsvorbereitung

Software Security

- Sicherer Software-entwicklungsprozess
- Threat Modeling & Architekturreviews
- Application & Mobile App Pentesting
- Quellcode-Audit
- CI/CD Audit

https://www.sba-research.org/professional-services/

Wer sind wir?

Nicolas Petri

Information Security Consultant

Security Awareness, Governance & Compliance

Seit 2018 bei SBA

Gerald Sendera

Legal Counsel & Datenschutzverantwortlicher

Legal Security & Datenschutz-Compliance

Seit 2017 bei SBA

Ich wollte nur Software bauen – und jetzt mach ich CRA-Compliance

Konformität und Cybersicherheitsanforderungen (CRA Anhang 1 Teile I und II)

Bundesministerium Innovation, Mobilität und Infrastruktur
Bundesministerium Wirtschaft, Energie und Tourismus
FFG Forschung wirkt.
wirtschaftsagentur wien
Für die Stadt Wien
European Commission
FWF Österreichischer Wissenschaftsfonds
netidee FÖRDERUNGEN

[WID-SEC-2024-2048] Yubico YubiKey: Schwachstelle ermöglicht Klonen von Signaturschlüsseln

CVSS Base Score	CVSS Temporal Score	Remoteangriff	Datum	Stand	Mitigation
4.9 (mittel)	4.3 (mittel)	nein	04.09.2024	UPDATE 02.12.2024	ja

Betroffene Systeme

Betriebssystem

- Hardware Appliance

Produktbeschreibung

Die YubiKey Produktfamilie bietet Lösungen für eine Zwei-Faktor-Authentisierung.

Produkte

04.09.2024

- Yubico YubiKey 5 Series <5.7
- Yubico YubiKey 5 FIPS <5.7
- Yubico YubiKey 5 CSPN <5.7
- Yubico YubiKey Bio Series <5.7.2
- Yubico YubiHSM <2.4.0
- Yubico YubiHSM <2.4.0 FIPS

https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2024-2048

heise online heise+ entdecken

heise+ Newsticker IT & Tech Security KI Developer Entertainment Wisse

heise online > Security > Yubikey-Lücke: Hersteller will weder Update noch generell Ersatz bereitstellen

Yubikey-Lücke: Hersteller will weder Update noch generell Ersatz bereitstellen

Yubico plant auch künftig keine Firmware-Updates für verwundbare Yubikeys. Über einen Ersatz will das Unternehmen im Einzelfall entscheiden.

144

https://www.heise.de/news/Yubikey-Cloning-Angriff-Kein-Firmware-Update-vielleicht-Key-Austausch-9857807.html

ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

(2) Auf der Grundlage der Bewertung [redacted] digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,

b) mit einer sicheren Standardkonfigur[redacted] dem gewerblichen Nutzer in Bezug auf ein [redacted] abgeschneidetes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,

c) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Sicherheitsaktualisierungen [redacted] installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können;

d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden,

e) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel,

f) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen und deren Beschädigung melden,

g) die Verarbeitung person[redacted] auf solche, die angemessen und von Bedeutung sind, und auf das für die Zwe[redacted] Maß beschränken („Datenminimierung“);

h) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), sicherstellen,

i) die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,

j) so konzipiert, entwickelt und hergestellt werden, dass sie — auch bei externen Schnittstellen — möglichst geringe Angriffsflächen bieten,

k) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,

l) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen,

m) den Nutzern die Möglichkei[redacted] wenn diese Daten auf andere Pro[redacted] Weise geschieht.

Teil II Anforderungen an die Behandlung von Schwachstellen

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) Schwachstellen und [redacted] digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste [redacted] baren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wir[redacted]

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen teilen und veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Eleme[redacted] hen, sowie eindeutige und verständliche Informationen[redacted] ründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden;

(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für P[redacted] mit digitalen Elementen bereitstellen, damit Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen g[redacted] omatisch behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsp[redacted] fügung stehen, unverzüglich un[redacted] Bezug auf ein mabg[redacted] dukt mit digitalen [redacted] werden, zusammen mit Hin[redacted] einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R2847

Risikobewertung/Threat Modelling

„secure by default“

Sicherheitsupdates

Datenschutz/Datenminimierung

Datenschutz/Löschung/Portierbarkeit

SBOM

Pentests

Veröffentlichung

mehr Sicherheitsupdates

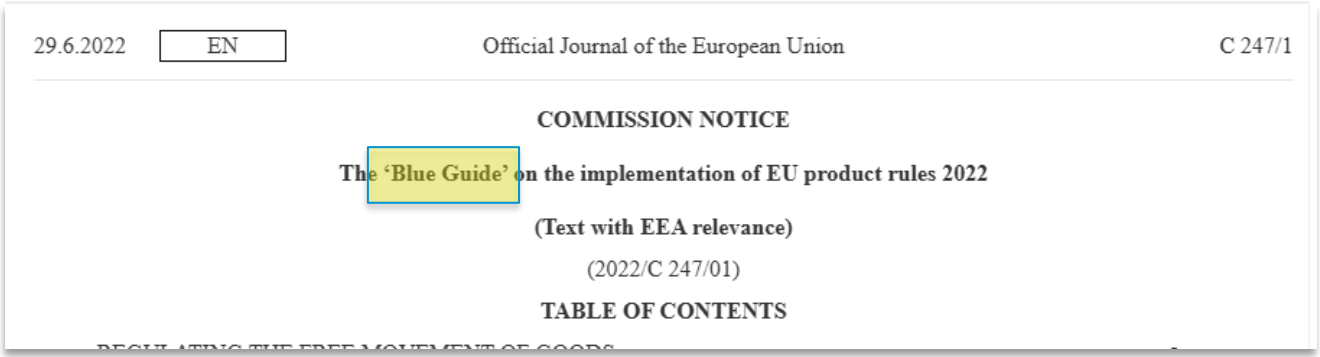
noch mehr Sicherheitsupdates

14 Requirements

8 Requirements

CRA = Konformitätsbewertung!

No CE-Mark – No EU-Market!



29.6.2022 EN Official Journal of the European Union C 247/1

COMMISSION NOTICE

The 'Blue Guide' on the implementation of EU product rules 2022

(Text with EEA relevance)

(2022/C 247/01)

TABLE OF CONTENTS

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022XC0629%2804%29&qid=1747224321757

90% aller Produkte

10% aller Produkte*

* https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-cyber-resilience-act

Standard	Wichtig Klasse I	Wichtig Klasse II	Kritisch
Selbstbewertung der Konformität (CE) möglich			
Eigenverantwortung auf Basis einer **Risikoabschätzung**	Selbstbewertung möglich nach standardisiertem Verfahren, **harmonisierten Normen** oder Schemata **SONST** - Konformitätsbewertung unter Beteiligung Dritter	Konformitätsbewertung unter Beteiligung Dritter (EU-Baumusterprüfung, interne Fertigungskontrolle, umfassende Qualitätskontrolle)	Konformitätsbewertung unter Beteiligung Dritter (europäisches Schema für die Cybersicherheitszertifizierung oder eines der Verfahren für Kl. II)
Alle Produkte, die nicht unter eine höhere Kategorie fallen	19 Produktgruppen	4 Produktgruppen	dzt. 3 Produktgruppen
	zB Browser, Passwortmanager, SIEM, VPN, Router, Modems, Switches, Netzwerkmonitore, „Virtuelle Assistenten“, Smart-Home-Devices, Wearables	zB Firewalls/IDS/IPS, Virtualisierungsumgebungen	Hardwaregeräte mit Sicherheitsboxen; Smart-Meter-Gateways in intelligenten Messsystemen; Chipkarten oder ähnliche Geräte

SBA Research, 2025

Alternative? Einstieg? Ansatz für die „90%“? https://owaspsamm.org/

niederschwellig

strukturiert

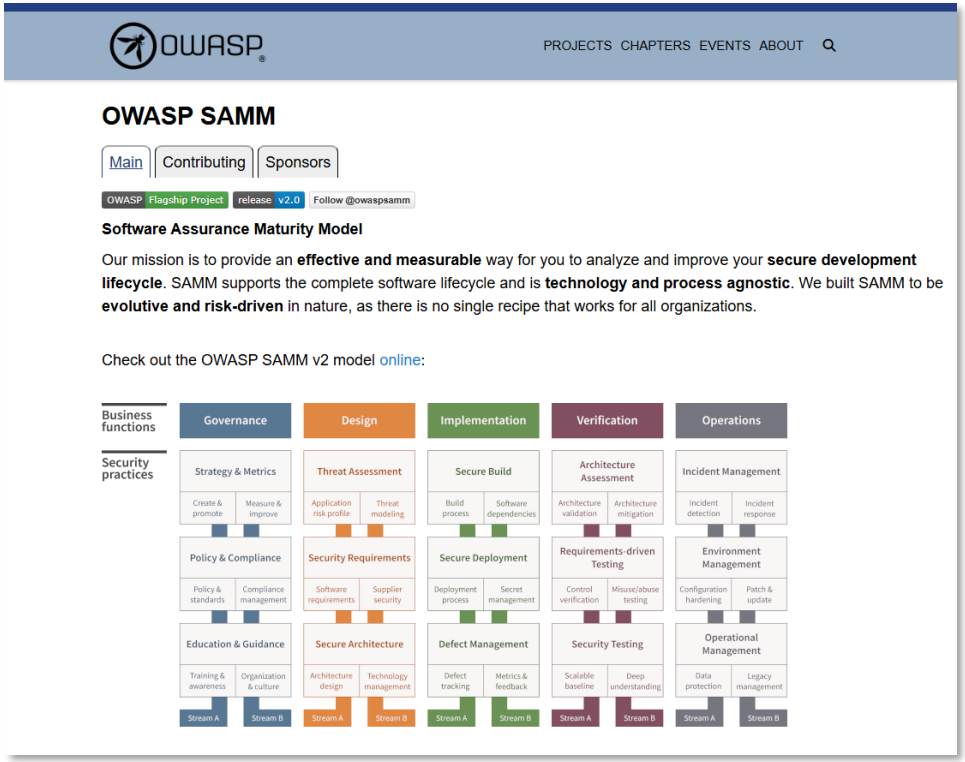
kostenlos

selbst anwendbar

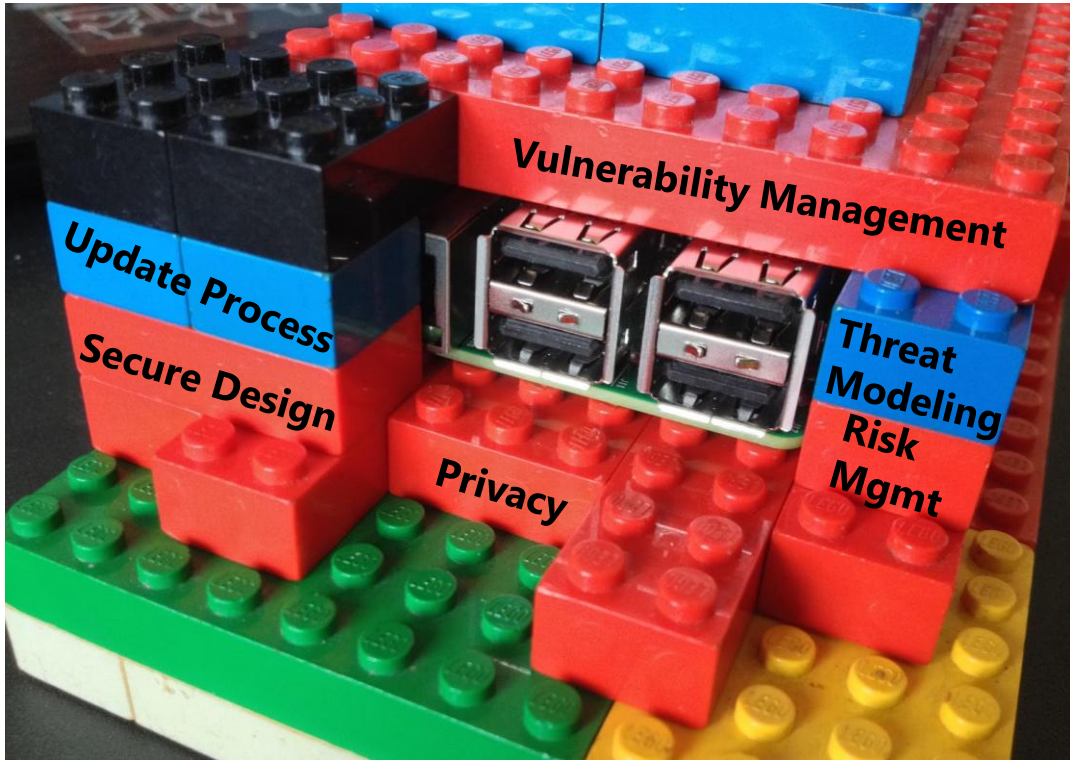
ABOUT US

This is an OWASP Project.
OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

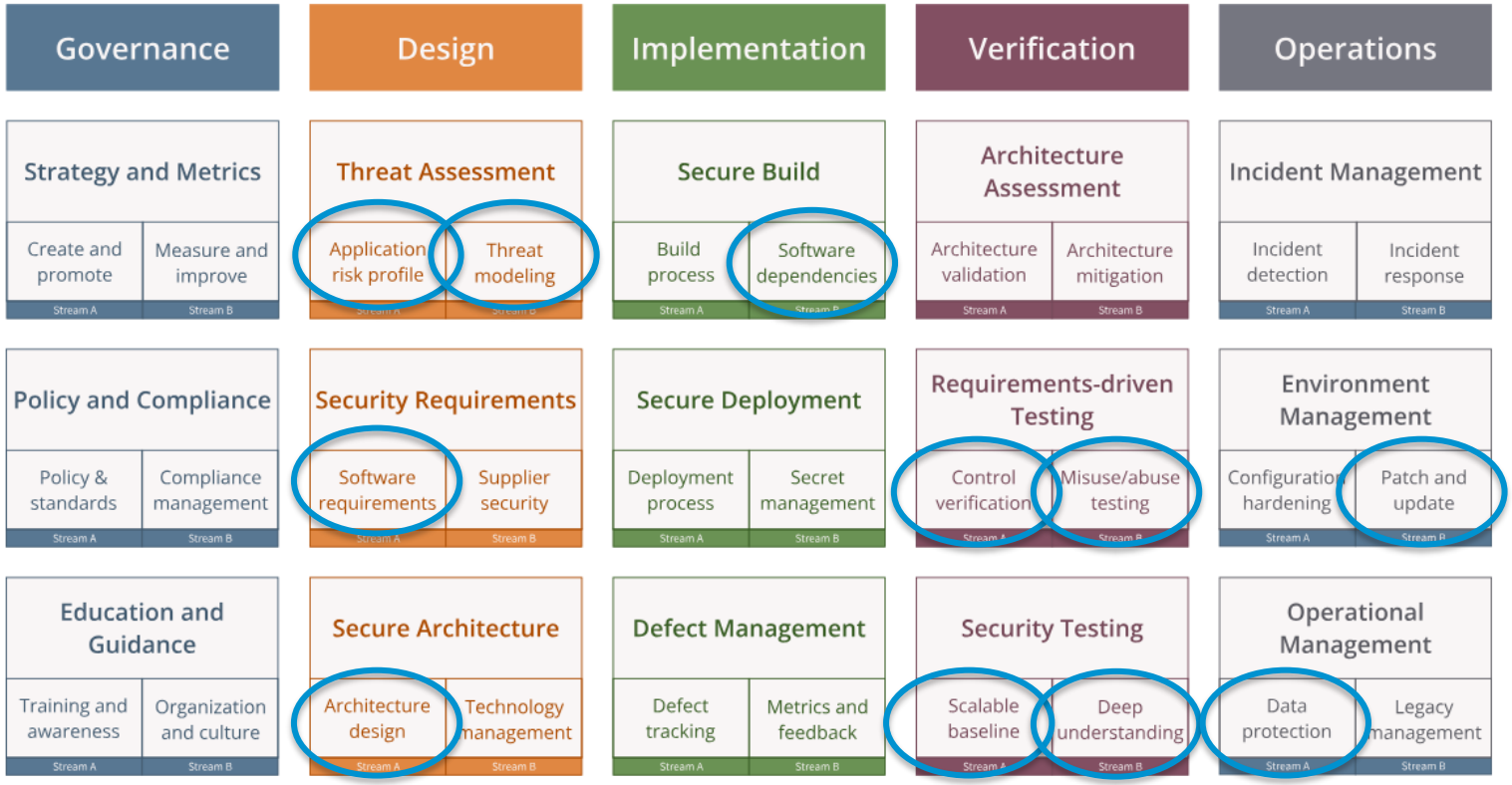
https://owaspsamm.org/about/



Was macht ein sicheres Produkt aus?



TL;DR: SDLC FTW



https://owaspsamm.org

SDLC Maturity

Model | Design | Threat Assessment

The Threat Assessment (TA) practice focuses on identifying and understanding of project-level risks based on the functionality of the software being developed and characteristics of the runtime environment. From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business.

By starting with simple threat models and building application risk profiles, an organization improves over time. Ultimately, a sophisticated organization would maintain this information in a way that is tightly coupled to the compensating factors and pass-through risks from external entities. This provides greater breadth of understanding for potential downstream impacts from security issues while keeping a close watch on the organization's current performance against known threats.

Maturity level		Stream A Application Risk Profile	Stream B Threat Modeling
1	Best-effort identification of high-level threats to the organization and individual projects.	A basic assessment of the application risk is performed to understand likelihood and impact of an attack.	Perform best-effort, risk-based threat modeling using brainstorming and existing diagrams with simple threat checklists.
2	Standardization and enterprise-wide analysis of software-related threats within the organization.	Understand the risk for all applications in the organization by centralizing the risk profile inventory for stakeholders.	Standardize threat modeling training, processes, and tools to scale across the organization.
3	Proactive improvement of threat coverage throughout the organization.	Periodically review application risk profiles at regular intervals to ensure accuracy and reflect current state.	Continuously optimization and automation of your threat modeling methodology.

https://owaspsamm.org/model/design/threat-assessment/

Output
Scoring

- **Was bekommt man?**
  - quantitative Bewertung aller Bereiche
  - Blinde Flecken leicht zu identifizieren
- **Schlüsselergebnisse eines Assessment**
  - Ist-Stand
  - Roadmap & Motivation für kurz- und langfristige Weiterentwicklung
  - Die *„Wo soll ich anfangen?“*-Hilfe und Guidance für einfache Verbesserungen

		Current Maturity Score			
			Maturity		
Functions	Security Practices	Current	1	2	3
Governance	Strategy & Metrics	0,63	0,25	0,25	0,13
Governance	Policy & Compliance	0,63	0,50	0,13	0,00
Governance	Education & Guidance	0,75	0,38	0,13	0,25
Design	Threat Assessment	0,50	0,25	0,25	0,00
Design	Security Requirements	0,25	0,25	0,00	0,00
Design	Secure Architecture	0,88	0,50	0,13	0,25
Implementation	Secure Build	1,88	1,00	0,63	0,25
Implementation	Secure Deployment	1,13	0,75	0,38	0,00
Implementation	Defect Management	0,63	0,63	0,00	0,00
Verification	Architecture Assessment	0,88	0,75	0,00	0,13
Verification	Requirements Testing	0,75	0,25	0,25	0,25
Verification	Security Testing	1,50	0,75	0,50	0,25
Operations	Incident Management	0,13	0,13	0,00	0,00
Operations	Environment Management	0,50	0,38	0,13	0,00
Operations	Operational Management	1,25	1,00	0,13	0,13

DIE 3 zum Mitnehmen

1. **Produktklassen erheben** – (CRA ANHANG III) inkl. Bonusfrage: „ist es ein Produkt??“

2. **SDLC etablieren / SAMM Assessment durchführen** – Best Practices folgen

3. **Vorbereitet sein** – für alle Eventualitäten

SBA Research
Professional Services

Security Governance

- Security Governance Lagebild
- ISMS / ISO 27001
- Compliance (NIS-2, CRA, DORA, etc.)
- Risikomanagement & Business-Impact
- Audit & Beratung

Cyber Defense

- Cyber Security Lagebild
- Penetrationstests (Infrastruktur, Cloud, Netzwerk)
- Red/Blue/Purple Teaming
- Social Engineering & Phishing
- SWIFT CSP Audit

Security Schulungen

- Security Awareness
- Hacking & Defense (Web, Windows, IoT)
- Secure Coding & Application Security
- Cloud & Cloud-Native Security
- Zertifizierungsvorbereitung

Software Security

- Sicherer Software-entwicklungsprozess
- Threat Modeling & Architekturreviews
- Application & Mobile App Pentesting
- Quellcode-Audit
- CI/CD Audit

https://www.sba-research.org/professional-services/

Contact Information

Gerald Sendera
gsendera@sba-research.org

Nicolas Petri
npetri@sba-research.org

SBA Research gGmbH
Floragasse 7
1040 Wien