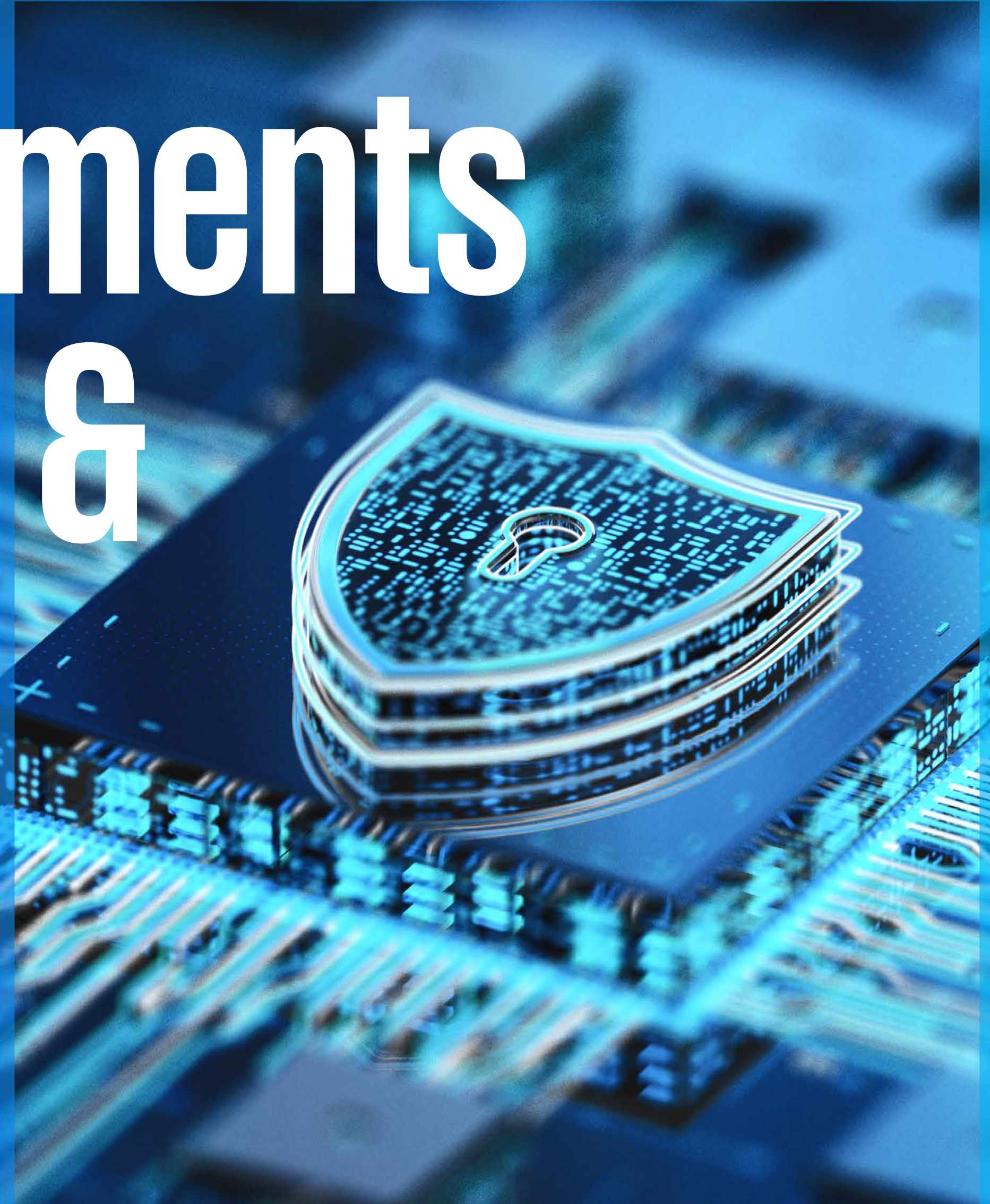




Security Requirements Engineering & Architecture



Security Requirements Engineering & Architecture

Die zunehmende Komplexität der Bedrohungslandschaft, regulatorische Anforderungen und die rasante Entwicklung neuer Technologien erfordern eine proaktive und umfassende Betrachtung der Informationssicherheit.

Security Requirements Engineering & Architecture übersetzt Geschäftsziele und Risiken in klare, überprüfbare Anforderungen und setzt sie in konsistente, skalierbare Cloud- und On-Prem-Architekturen um. Durch Threat Modeling, Priorisierung und verbindliche Architekturprinzipien entstehen belastbare Designs, die Compliance unterstützen und Angriffsflächen reduzieren.

Das Ergebnis ist eine messbare, effiziente und zukunftsfähige Sicherheitsarchitektur, die Risiken zielgerichtet adressiert und Investitionen wirksam macht.

Kommt Ihnen eine dieser Situationen bekannt vor?

- **Architekturprinzipien, Richtlinien** und **Kontrollen** sind **nicht konsequent etabliert** oder fehlen vollständig.
- **Threat Modeling** findet **nicht** statt oder nur punktuell und zu spät.
- Sie haben **nicht genügend qualifizierte Security-Architekten** und Requirement Engineers für die Umsetzung ihrer Projekte.
- Sie haben **Probleme** bei der **Auswahl** eines geeigneten **MSSP**.
- Es **fehlen klar formulierte, priorisierte** und **überprüfbare Security Requirements** entlang des gesamten Produkt- und Service-Lebenszyklus.
- **DevSecOps** und **Secure-by-Design-Praktiken** sind **nicht etabliert**.

Ohne klare Security Requirements und architektonische Leitplanken bleibt Security reaktiv, inkonsistent und teuer.

Wir verstehen, dass jedes Unternehmen einzigartig ist und spezifische Bedürfnisse und Herausforderungen hat. Daher bieten wir maßgeschneiderte Lösungen, die auf die individuellen Anforderungen Ihres Unternehmens abgestimmt sind.

Dabei arbeiten wir eng mit Ihrem Team zusammen, um sicherzustellen, dass Ihre Bedürfnisse optimal umgesetzt werden.

Wir helfen Ihnen, Ihre Sicherheitsausgaben zu optimieren, sodass Ihre Investitionen in die Informationssicherheit maximalen Nutzen bringen.

Mit unserer umfassenden Beratung und Unterstützung sind wir Ihr Partner bei der Entwicklung von Security-Architekturen, die nicht nur den aktuellen Anforderungen entsprechen, sondern auch auf zukünftige Herausforderungen vorbereitet sind.

Unser Ansatz: Strategie, Struktur und Erfolg

Unsere Experten im Bereich Security Requirements Engineering & Architecture unterstützen Sie bei der Definition und Erarbeitung individuell maßgeschneiderter Lösungen, um Risiken zu minimieren.

Die Zusammenarbeit mit KPMG macht den Unterschied:

- Anpassungsfähig: Wir entwickeln maßgeschneiderte Lösungen für jeden unserer Kunden. „One-Size-fits-all“ gibt es bei uns nicht.
- Risikominderung: Wir beugen Sicherheitsverletzungen vor – durch umfassende Bewertungen, Schwachstellenidentifikation und Lösungsempfehlungen.
- Compliance: Wir unterstützen unsere Kunden bei der Umsetzung von branchenspezifischen und regulatorischen Anforderungen.
- Kosteneffizienz: Wir arbeiten mit unseren Kunden zusammen, um Lösungen zu entwickeln, die Security und Ausgaben in Einklang bringen.
- Expertise: Wir punkten mit der Kompetenz unserer Mitarbeiter:innen. Deren Erfahrung und spezifisches Know-how wird ständig durch neue Zertifizierungen gefördert.

Unsere Leistungen im Überblick:



MDM-Konzeption

Wir entwickeln Richtlinien für Enrollment, Compliance und App-Management, definieren Hardening-Baselines und integrieren MDM in IAM/EDR-Prozesse für sicheren Geräteinsatz.



Cloud-Security-Architektur

Wir unterstützen beim Entwurf sicherer Cloud-Zielarchitekturen mit Landing Zones, IAM, Netzwerksegmentierung, Schlüsselmanagement, Logging und Policies und liefern Guardrails sowie IaC-Patterns für skalierbare Umsetzung.



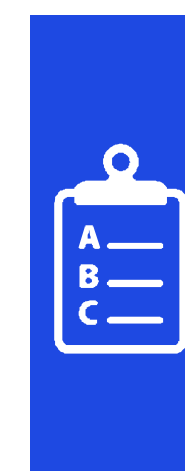
Unterstützung bei der Auswahl der MSSP-/Security-Tools

Wir unterstützen bei der Definition von Anforderungen, vergleichen Anbieter, steuern PoCs/RfPs, bewerten Wirtschaftlichkeit und planen für passgenaue Entscheidungen.



Cloud Security Assessments

Analyse von Cloud-Konfigurationen gegen Best Practices und Benchmarks (z. B. CIS). Identifikation von Fehlkonfigurationen, Risikobewertung und konkreter Maßnahmen-/Remediation-Fahrplan.



Security Requirements Engineering

Wir leiten überprüfbare Security Requirements aus Risiken und Compliance ab, priorisieren sie und verankern sie nachvollziehbar im SDLC – inklusive Akzeptanzkriterien und Traceability.



IT Service Management für Security

Definition von Security-Services, SLAs und Prozessen (Incident/Request/Change). Aufbau von Servicekatalog, Workflow-Automatisierung und Reporting, z. B. mit ServiceNow/Jira für auditable Security-Operations.



DLP-Konzeption

Wir ermitteln Schutzbedarf, klassifizieren Daten, gestalten Policies für Endpunkte, E-Mail und Cloud, evaluieren Tools und planen Betrieb und Rollout für wirksamen Datenabfluss-Schutz.

KPMG.
Make the
Difference.

Kontakt

Für weitere Informationen wenden Sie sich bitte an einen unserer Experten oder besuchen Sie uns unter [kpmg.at](https://www.kpmg.at).

Daniel Kroiss

Partner

M +43 664 889 854 78
dkroiss@kpmg.at

Josef Marold

Manager

M +43 664 888 292 19
jmarold@kpmg.at

[kpmg.at](https://www.kpmg.at)

