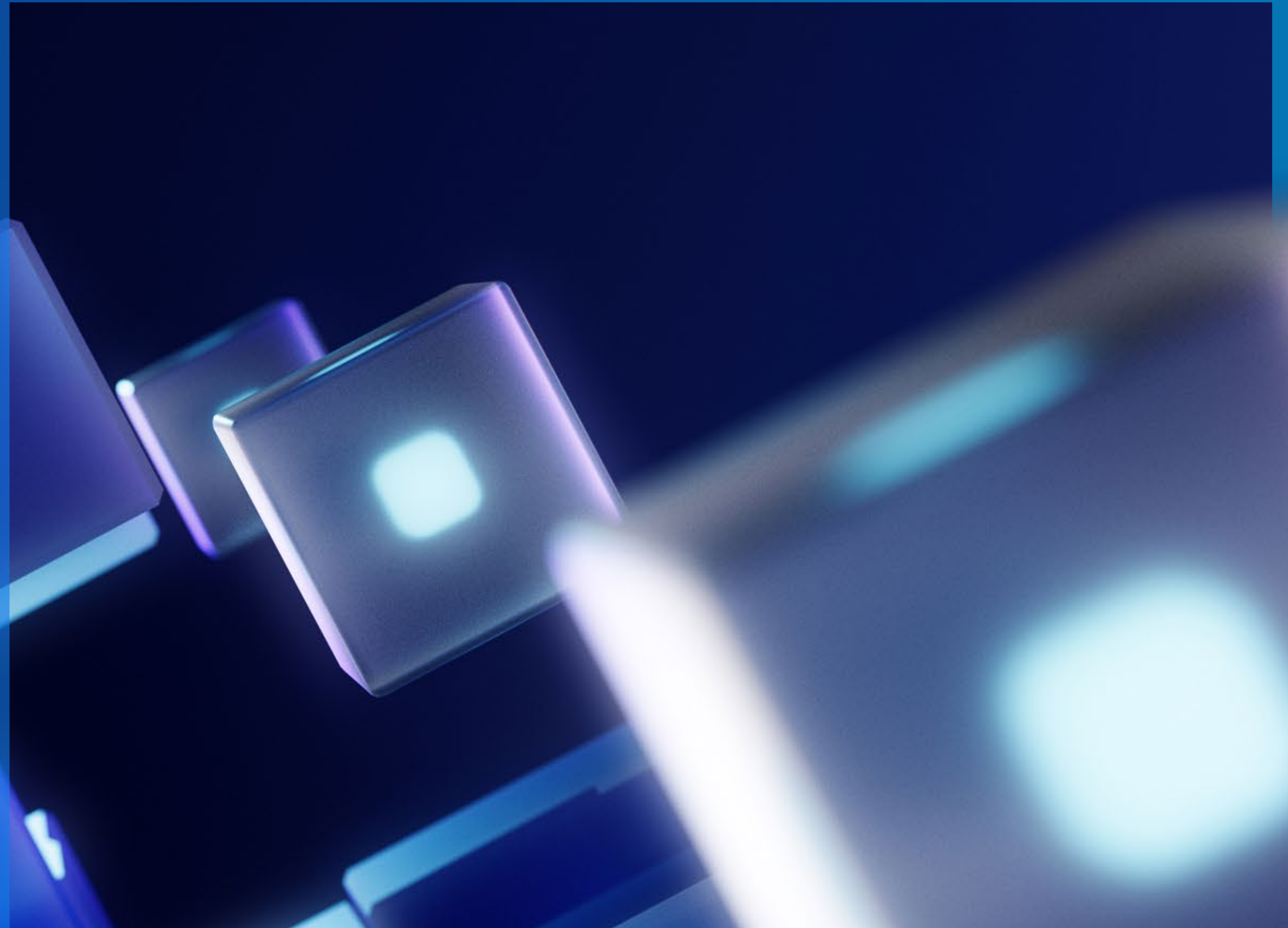


Security Testing

Das Fitnessprogramm für
widerstandsfähige IT-Systeme



Security Testing

Sicherheitstests sind ein unerlässliches Mittel, um digitale Prozesse resilient zu betreiben.

Unsere Expert:innen bewerten die Sicherheit Ihrer Systeme, ermöglichen eine Qualitätsverbesserung und vermeiden so Sicherheitsvorfälle.

Zudem fordert die aktuelle Cybersecurity-Regulatorik (NIS-2, CRA, DORA etc.) Sicherheitstests, insbesondere für kritische IT-Systeme und -Anwendungen.

Digitale Qualitätssicherung

Die komplexen IT-Systeme moderner Unternehmen sind die Grundpfeiler der Digitalisierung, entsprechend resilient müssen diese gestaltet sein. Security Testing ist ein essenzieller Baustein davon. Die Expert:innen von KPMG unterstützen Sie dabei, Ihre IT-Systeme in Bestform zu bringen und Schwachstellen zu finden, bevor andere es tun.

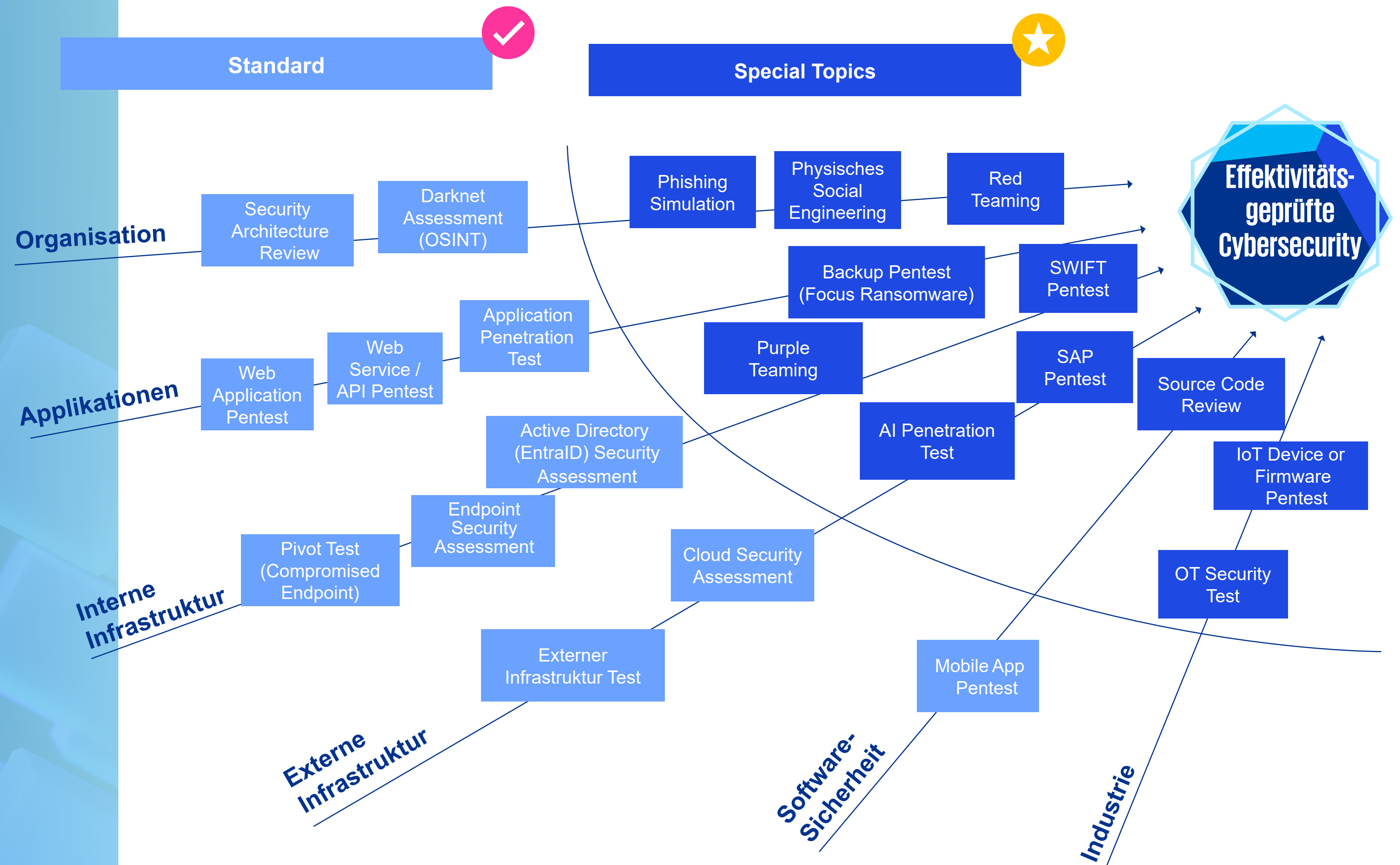
Wir helfen Ihnen, die Ergebnisse der Security-Tests zielgruppengerecht aufzubereiten und die Risiken für Entscheidungsträger adäquat darzustellen.

Wissensweitergabe & ressourcenschonender Ablauf

Die Wissensweitergabe an Ihre interne Organisation ist von zentraler Bedeutung, nur so können die erkannten Verbesserungsmaßnahmen langfristig wirken. Nach der Ergebnisbesprechung unterstützen wir Sie dabei, die Maßnahmen mit Ihrem IT-Betrieb oder mit den Software-Entwickler:innen umzusetzen.

Testkategorien

Das KPMG Security Testing Team ist Ihr vertrauenswürdiger Partner für alle Arten von Sicherheitstests. Durch das KPMG Netzwerk greifen wir auf Expert:innen in allen relevanten Technologien zurück, wie z. B. Spezialisierungen auf Mainframe Security Testing oder SAP Penetration Tests. Durch unser breites Branchenverständnis können wir neben rein technischen Tests auch umfassendere Assessments wie Prozessanalysen oder IT-Analysen durchführen.



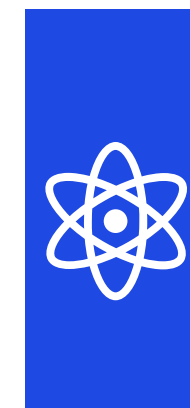
Wir bieten Ihnen unter anderem folgende Arten von Security-Tests:

- ▶ **Web Application Penetration Test**
- ▶ **AI Penetration Test**
- ▶ **Red Teaming / TLPT / TIBER-AT**
- ▶ **Purple Teaming**
- ▶ **Netzwerk Penetration Test**
- ▶ **Ransomware Safe Back-up Assessment**
- ▶ **SAP Penetration Test**
- ▶ **OT Penetration Test**

Ihre Vorteile:

- Hochqualitative Security-Tests
- Alle Security-Tester:innen verfügen über anerkannte Zertifikate (OSCP, SANS/GIAC etc.)
- Friktionsfreie Zusammenarbeitsmodelle mit raschen Test-Abrufen
- Weitere Leistungen wie Schulungen oder Unterstützung bei der Fehlerbehebung

Unsere Leistungen im Überblick:



Security-Tests

Die Durchführung von einzelnen ad-hoc Security-Tests stellt den klassischen Ansatz dar. Wir helfen Ihnen durch einen reibungslosen Ablauf, das Projekt durchzuführen, damit Sie Ihre internen Ziele erreichen können.



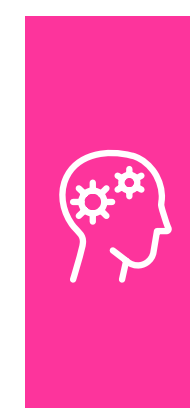
Penetration-Testing-Jahresplanung

Wir unterstützen Sie bei der Planung und Durchführung von mehreren Tests, beispielsweise wenn Sie durch eine Regularität wie z. B. DORA zu gewissen jährlichen Tests verpflichtet sind.



Security-Testing-Prozess

Wir etablieren mit Ihnen gemeinsam einen sinnvollen Security-Testing-Prozess inkl. Vorgabedokumente. Ziel ist eine gute Einbettung in schon vorhandene Schwesterprozesse wie Schwachstellen- oder Patchmanagement.



Awareness-Maßnahmen & -Trainings

Wir führen für Sie zielgruppenspezifische Trainings für Entwickler:innen und andere Mitarbeiter:innengruppen durch. Darunter fallen auch gezielte Phishing-Simulationen, um die Robustheit der Organisation zu testen.



TIBER AT / TLPT

Die Durchführung von TIBER AT Tests verlangt ein sehr strukturiertes Vorgehen. Wir helfen Ihnen bei der Navigation durch einen TIBER AT / TLPT Test und führen sowohl die Threat Intelligence als auch die Red-Teaming-Phasen durch. Auf Wunsch setzen wir mit Ihnen im Vorfeld Ihren internen Prozess entsprechend auf.



Begleitung bei Maßnahmenumsetzung

Ein Security-Test alleine verbessert nichts. Wir unterstützen ihre Entwickler:innen oder IT-Betriebsmitarbeiter:innen in der Umsetzung der Detailmaßnahmen und können so eine raschere und saubere Umsetzung ermöglichen.



Automatisierung durch Breach & Attack Simulation

Für gewisse Organisationen ist z. B. ein jährlicher Test oftmals zu wenig. Durch den Einsatz von „Breach & Attack Simulation“ (BAS) oder KI-basierte Werkzeuge kann als Ergänzung die Durchführung gezielter Angriffe laufend getestet werden. Wir unterstützen Sie in der Auswahl der geeigneten Software oder betreuen die Software für Sie.

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).

Severin Winkler

Director

M +43 664 820 24 24
severinwinkler@kpmg.at

Benjamin Petermaier

Senior Manager

M +43 664 88829161
bpetermaier@kpmg.at

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



© 2026 KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.