ALLGEIER CyRis

Pentesting as a Service

Strategischer Nutzen, Grenzen und richtige Erwartungshaltung

In diesem Whitepaper erfahren Sie:

- **was „as a Service“ bei Penetrationstests in der Praxis bedeutet – und woran es nicht zu erkennen ist,**
- **wo wiederkehrende Tests den größten Nutzen stiften,**
- **welche Grenzen Pentesting hat (insbesondere im Vergleich zu SOC/MDR),**
- **wie Sie Scope, Stakeholder und Qualität so steuern, dass Ergebnisse vergleichbar werden,**
- **wie Sie Erkenntnisse in Risikosteuerung und Nachweis der kontinuierlichen Verbesserung überführen.**

Hinweis: Dieses Dokument dient der Orientierung und ersetzt keine Rechtsberatung. Begriffe wie „Compliance“ und „Nachweis“ beziehen sich auf organisatorische Fähigkeiten und Dokumentation, nicht auf rechtliche Garantien.

Zielgruppe: CISO, IT-Leitung, Geschäftsführung, Compliance

Inhalt

Managed Summery

Pentesting as a Service (PTaaS) beschreibt keinen „anderen“ Penetrationstest, sondern eine andere Betriebs- und Vertragslogik: Sie vereinbaren ein Jahreskontingent und rufen einzelne Tests bei Bedarf ab – ohne jedes Mal das vollständige Projekt-Setup (Angebote, Verträge, Budgetierung, Zugänge) neu aufzusetzen.

Der größte Nutzen entsteht für Organisationen, die ohnehin mehrere Pentests pro Jahr durchführen – typischerweise in regulierten Umfeldern oder in Teams mit agiler Softwareentwicklung und hoher Change-Frequenz. PTaaS reduziert den organisatorischen Overhead und ermöglicht, Tests schneller und planbarer „on demand“ zu starten.

PTaaS ist ein planbarer Prüf- und Verbesserungsmechanismus: Er hilft, Sicherheitsannahmen regelmäßig zu verifizieren, Schwachstellen priorisiert abzuarbeiten und Fortschritt über Retests nachvollziehbar zu machen. Im Kern kommt man mit PTaaS über einen längeren Zeitraum auf ein gutes Sicherheitsniveau.

Damit PTaaS wirkt, braucht es ein klares Abruf- und Scope-Setup (Intake, Regeln, Zugriffe), Stakeholder-Verbindlichkeit, Qualitätsregeln (Methodik, Evidenz, Retest) sowie ein Reporting, das Findings in priorisierte Maßnahmen und Verantwortlichkeiten übersetzt.

Einzelprojekt vs. PTaaS (organisatorischer Unterschied)

	Einzelprojekt	PTaaS (Servicevertrag)
Wofür genutzt?	Anlass-/Projektgetrieben	Kontingent und Abruf über das Jahr
Organisation	Briefing, Zugriffe, Termine je Projekt	Einmaliges Setup und standardisierte Intakte
Durchlaufzeit	Oft stark PM-getrieben (Meilensteine)	Kürzer, weil Vorarbeit wiederverwendet wird
Transparenz	Status meist punktuell (Meilensteine)	Laufende Sicht auf Fortschritt und Findings
Vergleichbarkeit	Möglich bei stabilem Scope	In der Praxis höher durch Baselines/Retests als Standard
Skalierung	Bei vielen Tests hoher Koordinationsaufwand	Skalierbarer Testbetrieb (mehrere Abrufe)

Hinweis: Wiederholende Tests sind auch projektbasiert möglich. PTaaS adressiert vor allem organisatorischen Overhead (Briefing, Beschaffung, Koordination) und die Abrufbarkeit.

I. Was „as a Service“ wirklich bedeutet: Betrieb statt Einzelprojekt

In vielen Unternehmen wird „as a Service“ mit „schneller“ oder „automatisierter“ gleichgesetzt. Im Kontext von Penetrationstests bedeutet es vor allem einen wiederverwendbaren Betriebsrahmen (Scope-Templates, abgestimmte Spielregeln, feste Ansprechpartner, definierte Abläufe) und die Möglichkeit, mehrere Tests über das Jahr auf Abruf zu starten.

Wiederkehrende Tests lassen sich auch projektbasiert organisieren – der entscheidende Unterschied von PTaaS ist der deutlich geringere Projekt-Overhead.

Kernaussagen

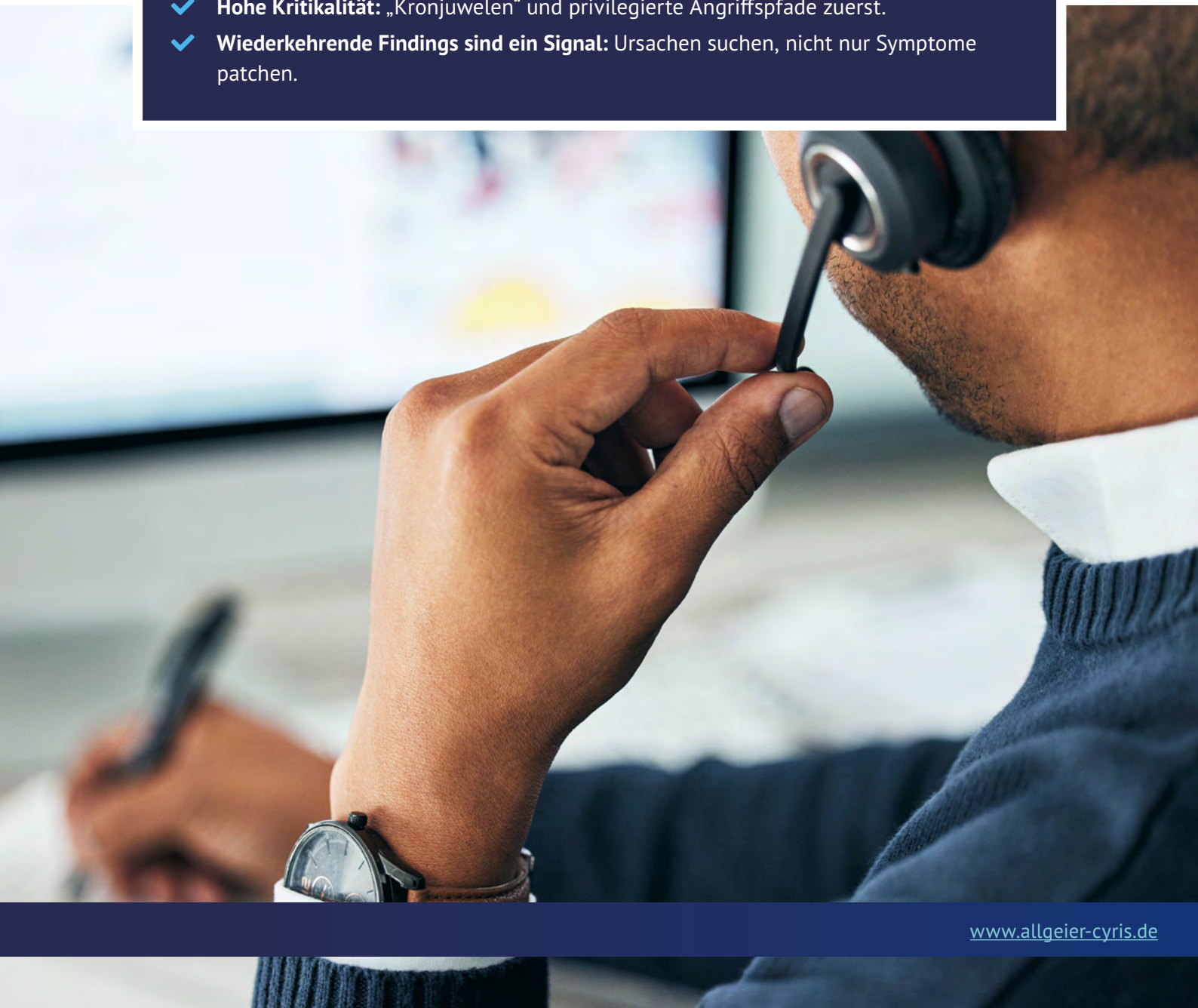
- **Service-Logik heißt:** Jahreskontingent vereinbaren, standardisiertes Intake nutzen und Tests bei Bedarf abrufen (statt jedes Mal „von vorn“ zu planen).
- **Der Wert entsteht vor allem durch** weniger Projekt-Overhead und schnellere Durchläufe – besonders bei vielen Tests pro Jahr.
- **Vergleichbarkeit, Retests und Trend-Sichten bleiben wichtig** – sie sind Ergebnis guter Betriebsführung, nicht das alleinige Unterscheidungsmerkmal.

II. Geeignete Ziele: Wo wiederkehrende Tests den größten Nutzen stiften

Nicht jede Umgebung braucht die gleiche Testfrequenz. Hohe Wirksamkeit erzielen wiederkehrende Tests dort, wo Angriffsflächen dynamisch sind oder wo privilegierte Angriffspfade den größten Nutzen für Kriminelle haben.

Kernaussagen

- **Hohe Change-Dynamik:** Web/API, Cloud-Konfigurationen, Identity, Integrationen.
- **Hohe Kritikalität:** „Kronjuwelen“ und privilegierte Angriffspfade zuerst.
- **Wiederkehrende Findings sind ein Signal:** Ursachen suchen, nicht nur Symptome patchen.

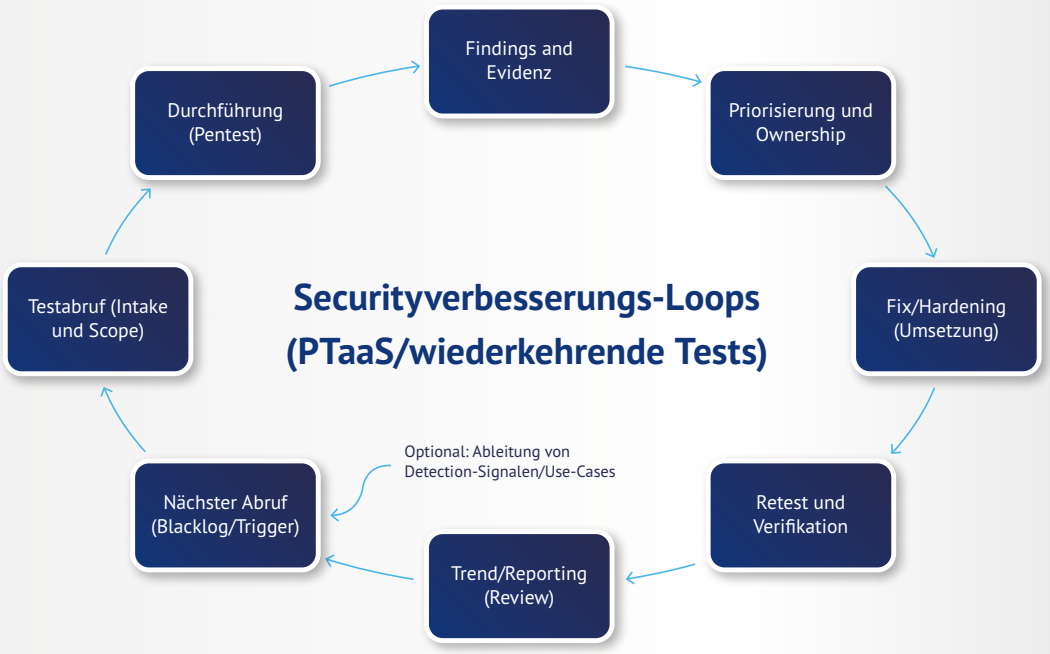


III. Einordnung im Sicherheits-programm: Welche Rolle PTaaS übernimmt

Pentesting as a Service (PTaaS) ist eine Betriebsform für wiederkehrende Sicherheitsprüfungen. Der Nutzen entsteht dadurch, dass Prüfungen schnell abrufbar sind, Ergebnisse vergleichbar bleiben und Verbesserungen über Retests nachvollziehbar werden. PTaaS stärkt damit Planbarkeit, Priorisierung und Umsetzungswirksamkeit im technischen Risikomanagement.

Kernaussagen

- **PTaaS macht wiederkehrende Prüfungen abrufbar und steuerbar** (Jahreskontingent, standardisiertes Intake, wiederverwendbare Scopes).
- **Es liefert die Grundlage für verbindliche Maßnahmenarbeit:** klare Ownership, Priorisierung, Retests und Trend-Reporting.
- **Der größte Effekt entsteht**, wenn Ergebnisse konsequent in Härtung, Release-Gates und die regelmäßige Re-Validierung überführt werden.



IV. Abruf- und Stakeholder-Modell: So bleibt PTaaS über das Jahr steuerbar

Ohne ein klares Abrufmodell wird PTaaS schnell zum Friktionspunkt: zu viele ad-hoc-Anfragen, wechselnde Prioritäten und unklare Zuständigkeiten pro Testabruf.

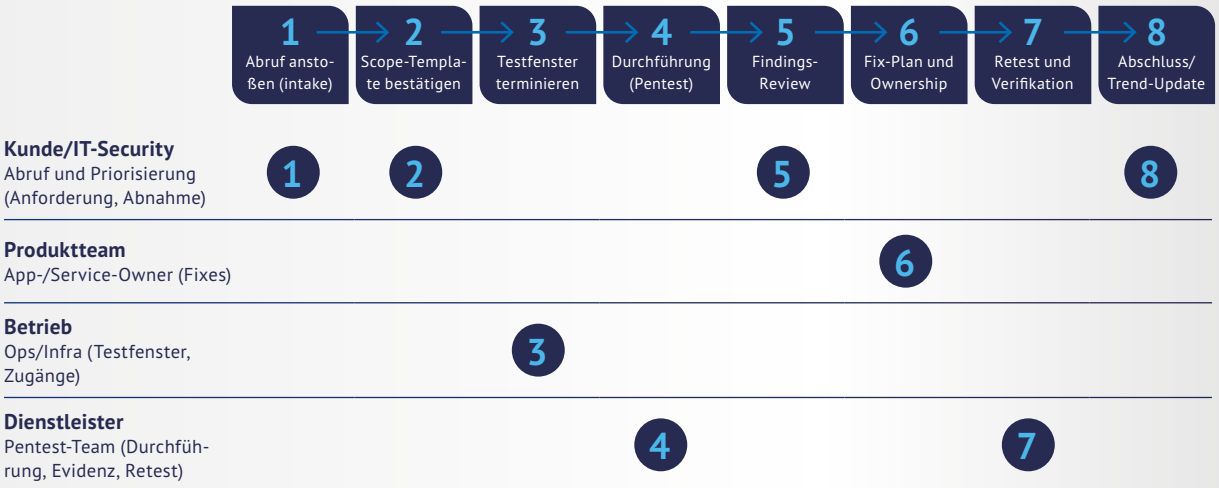
Steuerbarkeit entsteht nicht durch „mehr Regeln“, sondern durch wiederverwendbare Standards: ein einheitliches Intake, klare Scope-Templates, definierte Owner je Abruf und eine transparente Priorisierung innerhalb des Jahreskontingents.

Kernaussagen

- **Abruf statt Einzelprojekt:** Ein PTaaS-Setup definiert, wie Tests angefordert, priorisiert und gestartet werden (Intake -> Terminierung -> Durchführung -> Review) – wiederholbar für mehrere Abrufe im Jahr.
- **Scope-Templates als Standard:** In-Scope/Out-of-Scope, No-Go-Aktionen, Testfenster, Abhängigkeiten, Stop-Kriterien – als Vorlage, die pro Abruf nur noch angepasst wird.
- **Ownership und Koordination im Testbetrieb:** definierte Inputs je Rolle (Zugänge, Ansprechpartner, Change-Fenster) plus Deconfliction-Regeln und Eskalation bei Blockern (z. B. fehlende Zugänge, ungeplante Changes, instabile Umgebungen).

PTaaS-Abrufprozess – Wer liefert was?

Mehrere Abrufe über das Jahr, mit wiederverwendbaren Templates und definierten Übergaben



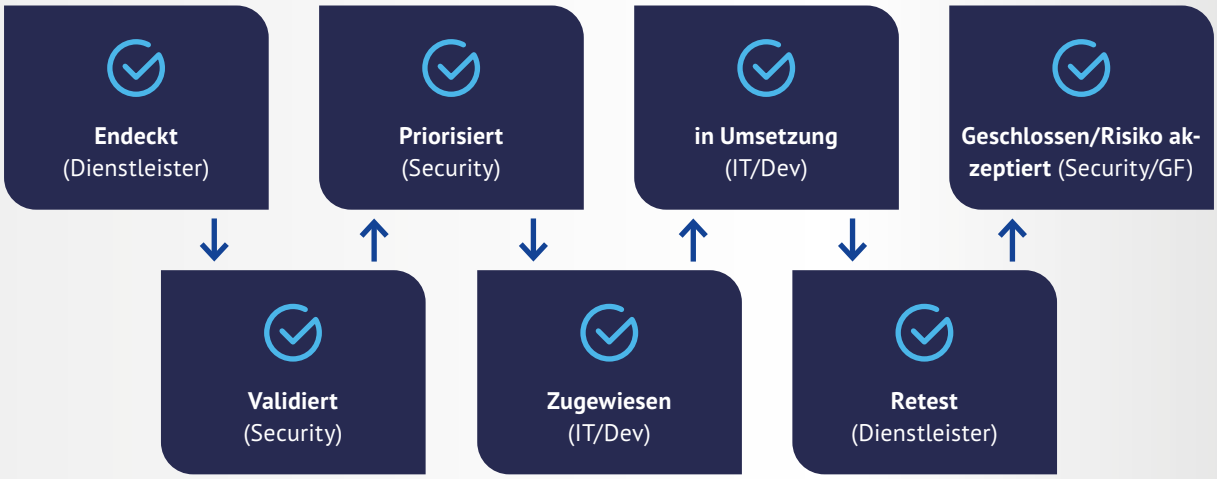
V. Qualität und Vergleichbarkeit: Methodik, Wiederholbarkeit, Retests

Der Nutzen eines Service-Ansatzes steht und fällt mit Qualität und Vergleichbarkeit. Das bedeutet: stabile Methodik, dokumentierte Regeln, und Retests als verbindlicher Bestandteil - nicht als optionales Add-on.

Kernaussagen

- **Methodik definieren** (z. B. Testansätze, Abdeckung, Evidenz, Risikoargumentation).
- **Wiederholbarkeit sicherstellen:** Baseline-Scopes, konsistente Schweregradlogik, klare Deliverables.
- **Retests als Pflicht:** Nur so wird Verbesserung nachweisbar und steuerbar.

Finding-Lifecycle



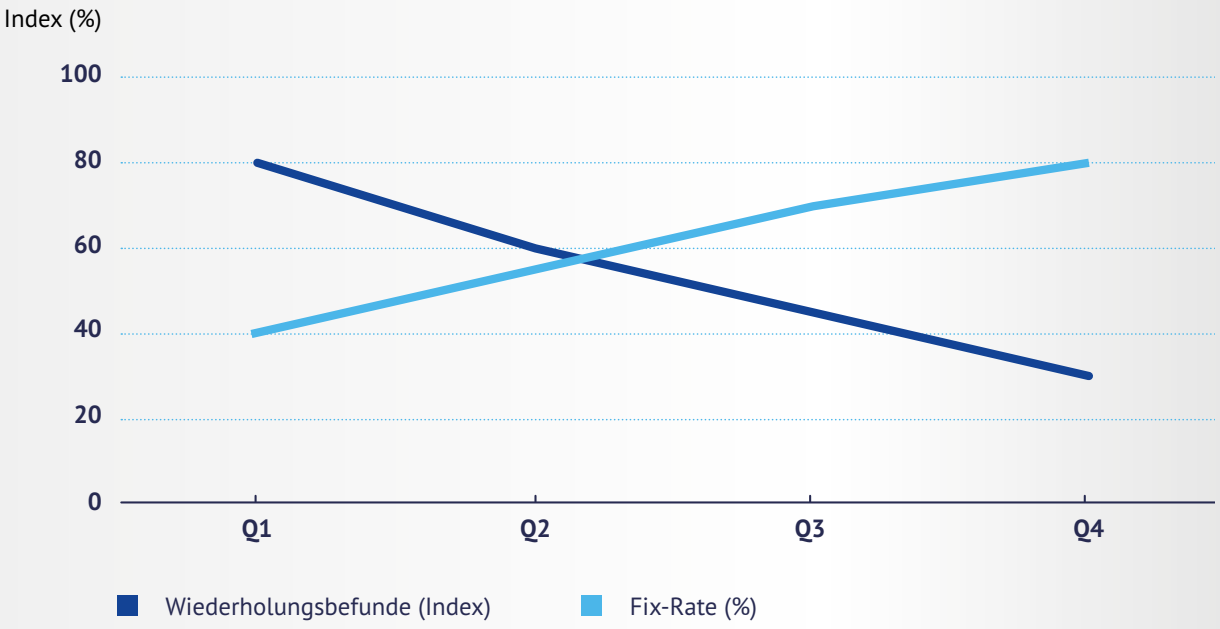
VI. Integration in Security-Steuerung: Risiko-Register, Maßnahmenplanung, Reporting

PTaaS entfaltet seinen Wert erst, wenn Findings nicht im PDF enden. Entscheider brauchen eine Übersetzung in Risiken, Maßnahmen und Prioritäten - inklusive Fortschrittsmessung.

Kernaussagen

- **Findings in ein Risiko-Register überführen:** Business-Impact, Eintrittswahrscheinlichkeit, Owner.
- **Maßnahmenportfolio statt Ticket-Flut:** bündeln, priorisieren, terminiert nachverfolgen.
- **Reporting nach Zielgruppe:** operativ (Teams) vs. taktisch (CISO) vs. strategisch (GF).

Beispiel-Reporting – Trend über Quartale



VII. Zusammenspiel mit Regulatorik (z. B. NIS-2): Kontinuierliche Verbesserung nachweisbar machen

Regulatorik fordert in der Praxis weniger „einmalige Maßnahmen“ als nachvollziehbare Betriebsfähigkeit: Risiko-orientierte Steuerung, dokumentierte Verbesserungen und die Fähigkeit, Wirksamkeit zu belegen.

Kernaussagen

- **PTaaS liefert Artefakte:** Scope, Evidenzen, Maßnahmenlisten, Retest-Nachweise, Trendberichte.
- **Wichtig: Nachweisbarkeit entsteht durch Prozess und Dokumentation** – nicht durch Formulierungen oder vermeintliche „Compliance-Garantien“.
- **Verknüpfen Sie Tests mit Change-Management:** große Änderungen sollten Retests auslösen.

VIII. Entscheidungsleitfaden: Wann lohnt sich der Wechsel von „Projekt“ zu „Service“?

Ein Wechsel lohnt sich, wenn Pentests nicht mehr nur „einmalig prüfen“, sondern als wiederkehrende Betriebsleistung genutzt werden sollen. Entscheidend sind zwei Fragen: Wie viele Tests benötigen Sie pro Jahr – und wie viel Aufwand entsteht heute durch Koordination über viele Einzelprojekte und ggf. mehrere Anbieter?

Kernaussagen

- **Wechsel-Indikatoren:** mehrere Pentests pro Jahr, hohe Change-Dynamik, wiederkehrende Findings, hoher Audit-/Steuerungsdruck – und eine fragmentierte Anbieterlandschaft (viele Einzelprojekte bei mehreren Dienstleistern).
- **Einstieg:** klein starten (Kronjuwelen), dann abrufbar erweitern (z. B. Releases, Integrationen, privilegierte Pfade).
- **Erfolgskriterium:** messbare Risikoreduktion, weniger organisatorischer Overhead und bessere Entscheidungsfähigkeit (Trend und Umsetzungsstatus statt Einzel-PDF).

Anhang: Templates und Checklisten

A1 – Scope-Briefing (One-Pager)

Nutzen: Ein einheitlicher Scope-One-Pager reduziert Reibung und macht Tests vergleichbar.

Feld	Beispielinhalt
Ziel / Zweck	z. B. Risiko in kritischen Benutzerpfaden reduzieren; Release-Readiness bestätigen
Testobjekte	Systeme/Apps/APIs, Umgebungen, URLs, IP-Bereiche, Accounts/Rollen
Scope-Grenzen	Out of Scope, No-Go-Aktionen, Zeitfenster, Stabilitätsanforderungen
Zugriffe & Voraussetzungen	Testaccounts, VPN, Whitelisting, Logs, Ansprechpartner
Deliverables	Management Summary, Findings + Risiko, Maßnahmenliste, Retest-Plan
Kommunikation	Eskalationsweg, Deconfliction, Kontaktliste, Stop-Kriterien

A2 – Kontingentnutzung über das Jahr (Beispiel-Taktung)

Hinweis: Das Beispiel dient nur zur Illustration eines Abruf- und Review-Rhythmus. In PTaaS entscheidet der Bedarf (Changes, Releases, Integrationen), wann welcher Test aus dem Kontingent abgerufen wird.

Quartal	Baseline-Tests	Erweiterungen	Retests / Review
Q1	Extern und Web/API (kritische Apps) Intern (repr. Standort/Netz)	Identity/Privileged Paths (Auswahl) Cloud-Konfiguration (kritische Accounts)	Findings aus Q4 Management-Review (Trend und Prioritäten)
Q2	Web/API (Release-getrieben)	Client/Endpoint (harter Pfad) Sondertests nach Changes	Findings aus Q1 Risiko-Backlog aktualisieren
Q3	Full-Scope Spotcheck (risikobasiert)	Third-Party/Integrationen (Auswahl)	Findings aus Q2 Status Maßnahmenportfolio
Q4	Baseline-Refresh (Kronjuwelen)	Planung nächstes Jahr	Findings aus Q3 Jahresabschluss und Plan

A3 – Entscheidungscheckliste: Projekt oder Service?

- ✔ Gibt es wiederkehrende Changes an kritischen Systemen (Release-Zyklen, Migrationen, neue Integrationen)?
- ✔ Brauchen Sie Vergleichbarkeit über Zeit (Trend, Fix-Rate, Wiederholungsbefunde)?
- ✔ Gibt es Audit-/Gremienbedarf für einen dokumentierten Verbesserungsprozess?
- ✔ Sind Owner für Maßnahmen und Retests benannt (IT, Produktteams, Betrieb)?
- ✔ Sind Scope-Grenzen und Spielregeln definiert, um Betriebsrisiken zu minimieren?
- ✔ Ist klar, wie Ergebnisse in Risiko-Register und Maßnahmenplanung übergehen?

Impressum / V.i.S.d.P.

Herausgeber: Allgeier CyRis GmbH · Hans-Bredow-Straße 60 · 28307 Bremen

Allgeier CyRis GmbH
Hans-Bredow-Straße 60
28307 Bremen

+49 (0) 421 706 242 1919
info@allgeier-cyris.de
www.allgeier-cyris.de