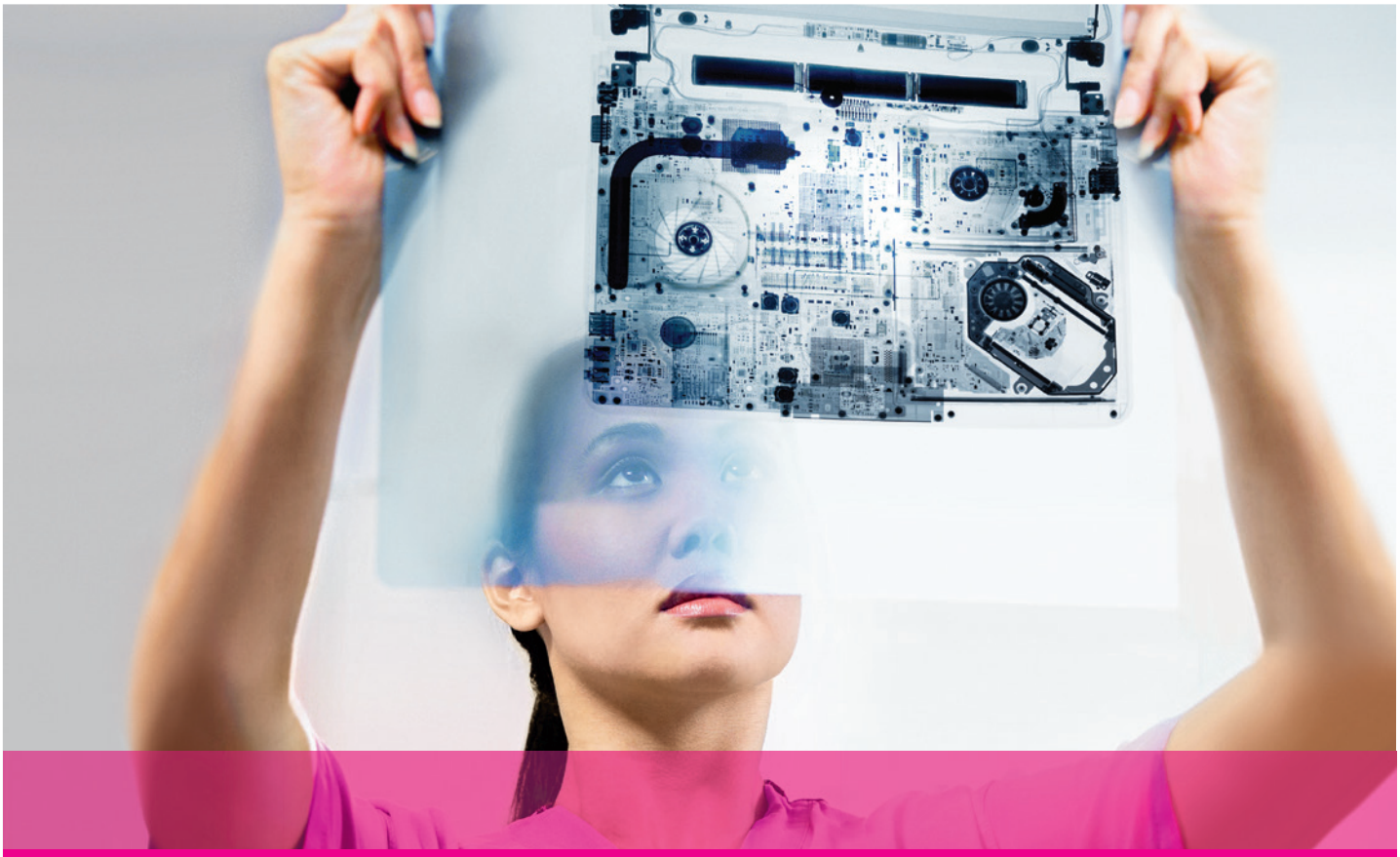


TESTING-AS-A-SERVICE.
WIR FINDEN SICHERHEITSLÜCKEN BEVOR HACKER ES TUN!

Das Thema IT-Sicherheit steht auf der Liste der IT-Prioritäten stets weit oben. Auch Sie benötigen Schutz vor dem Diebstahl hochsensibler Daten wie z. B. Firmengeheimnissen und möchten Ihre IT-Infrastruktur und Applikationen vor Angreifern / Hackern schützen?

Sie erwarten von Ihrem Testdienstleister enorme Flexibilität bei gleich bleibenden oder gar steigenden Qualitätsanforderungen?

Zugleich unterliegen Sie selbst einem hohen Kostendruck und müssen versuchen, Ihre Gesamtkosten transparent zu reduzieren?

Security-Testing (SEC) im Testing-as-a-Service(TaaS)-Modell von T-Systems bietet Penetrationstests und Security-Beratung zu kalkulierbaren Fest- und Stückpreisen und hilft Ihnen, diesen Herausforderungen erfolgreich zu begegnen und den Sicherheitslevel Ihrer Applikationen und Systeme um ein Vielfaches anzuheben.

Wählen Sie aus dem SEC-Servicekatalog der T-Systems, die für Ihren Bedarf passenden Pakete und Servicemodule und individualisieren Sie diese anhand der angebotenen Zusatzbausteine zu Ihrem kundenspezifischen Servicekatalog mit flexiblen Beauftragungsmöglichkeiten und kurzen Durchlaufzeiten. Durch einen hohen Grad an Standardisierung bei eindeutigen Eingangs- und Ausgangsbedingungen erfolgt die Leistungserbringung termingerecht und mit hoher Qualität.

Mit dem standardisierten TaaS-Modell können Sie die Ziele

- starke Service-Orientierung,
- SLA- und KPI-basiertes Liefermodell mit hohem Grad an Flexibilität,
- Abrechnung nach dem Pay-per-use(ppu)-Modell mit steigender Kostentransparenz

erfolgreich umsetzen. Sie erhalten so einen Service, der weit über das reine state-of-the-art Penetration-Testing hinausgeht.

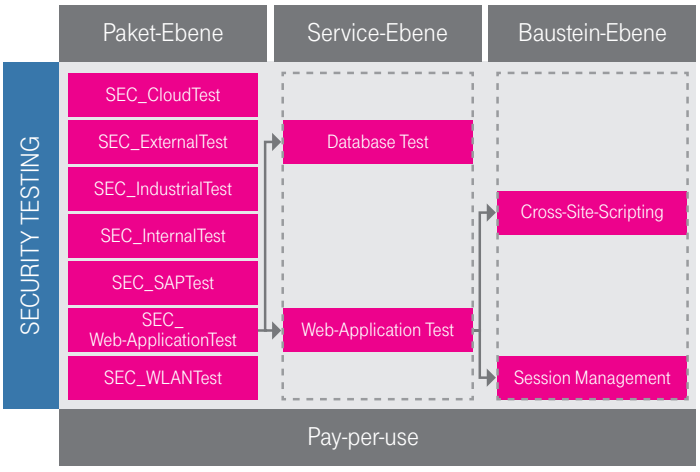
T · · Systems ·

SEC-PAKETE IM TAAS-MODELL.

- **SEC_CloudTest:**
  Security-Test von Applikationen auf der Cloud-Ebene (inkl. APIs und Webservices)
- **SEC_ExternalTest:**
  Security-Test von Applikationen, Netzwerk-Komponenten und IT-Systemen aus dem Internet (bzw. aus der Sicht eines Hackers)
- **SEC_IndustrialTest:**
  Security-Test von industriellen Anlagen und Steuerungssystemen inkl. Netzanbindung
- **SEC_InternalTest:**
  Security-Test von Applikationen, Netzwerk-Komponenten und IT-Systemen aus dem Intranet (bzw. aus der Sicht eines Innentäters)
- **SEC_SAPTest:**
  Security-Test der SAP Systeme und Applikationen (NetWeaver)
- **SEC_Web-ApplicationTest:**
  Security-Test von Web-Applikationen, angebundenen Datenbanken und Webservices
- **SEC_WLANTest:**
  Security-Test von WLANs, Access Points, Zugriffsmöglichkeiten und Abschottung zum internen Netzwerk

PAY-PER-USE-ELEMENTE VON SEC IM ÜBERBLICK.

Elemente des SEC-Service im Pay-per-use(ppu)-Modell.



KUNDENNUTZEN.

- **Risikominimierung** durch Erhöhung des **Sicherheitslevels** auf technischer und organisatorischer Ebene, sowie Nachweis eines vorhandenen **IT-Sicherheitslevels** durch einen unabhängigen Dienstleister.
- **Vertrauen** in die Sicherheit der Systeme durch die Umsetzung von Empfehlungen für effektive **Schutzmaßnahmen** gegenüber **Hacker-Angriffen.** Dabei **absolute Diskretion** beim Umgang mit den Ergebnissen des Tests. Sämtliche Maßnahmen werden **in enger Abstimmung** vorgenommen.
- **Effektive Tests,** die mit **Testmethoden** entworfen werden, die auf **Industriestandards** basieren.
- **Kostenminimierung** durch Bestellung bedarfsgerechter Kombinationen von Servicebausteinen, die sich an den **geschäftlichen Notwendigkeiten** orientieren.
- **Komplette Kostenkontrolle** und verursachergerechte Kostenzuordnung im **Pay-per-use-Modell.**

INPUT / OUTPUT.

Typische Ein- und Ausgaben für SEC ppu-Elemente.
Ihr Input: Zeitliche Rahmenbedingungen, Sicherheitsanforderungen, Dokumentation der Testobjekte, Pflichtenheft, Akkreditierungsvoraussetzungen
Unsere Leistung: Testspezifikation, Testkonzept, Testprotokoll, Reports, Empfehlungen, durchgeführter Security-Test

CREDENTIALS.

- **Testprojekte in folgenden Branchen:** Automotive, Telecommunications, Information Technology, Logistics & Transport, Public
- **Technologien:** SAP, Cloud, diverse Programmiersprachen (Java, C#, Python, Perl, ...), heterogene Systemlandschaften mit +20 Applikationen, +200 Systemen
- **Eingesetzte Werkzeuge:** Nessus, CORE Impact, Metasploit, Burp, Maltego, Netsparker, nmap, Nikto, w3af, T-Systems eigene Skripte und Tools

KONTAKT
Mailbox: Testing-Services@t-systems.com

T-Systems International GmbH
Marketing
Moltkestr. 2–6
78467 Konstanz, Deutschland

HERAUSGEBER
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main
Deutschland

Stand 06/2013 | Änderungen und Irrtümer vorbehalten | Papier chlorfrei gebleicht | typix