secunet redbox

Automotive Security –
Protect. Connect. Detect.

secunet

ECU Absicherung neu gedacht – Automatisierte Analyse von Schwachstellen

Die zunehmende Vernetzung von Fahrzeugen, verbunden mit komplexen Funktionen bis hin zum autonomen Fahren, geht einher mit einer steigenden Anzahl von Angriffsmöglichkeiten auf moderne Fahrzeuge. Damit verbunden sind erhebliche Manipulationen am Fahrzeug, die im schlimmsten Fall zur Beeinträchtigung der Fahrfunktionen führen können. Um diese Gefahren zu minimieren, ist es heutzutage unerlässlich, die zugrundeliegenden Systeme ausreichend zu härten, zu testen und vor Angriffen zu schützen.

Aus diesem Grund hat secunet die secunet redbox entwickelt.

Pentesting – Kein „nice to have“

Die steigende Relevanz des Pentestings spiegelt sich auch in geplanten Regulierungen und Standardisierungen wider. So sind z. B. in den USA Penetrationstests bereits heute vorgeschrieben und neben der SAE J3061, der ersten IT-Security-Norm für Fahrzeuge, auch im aktuellen Entwurf der entstehenden ISO 21434 enthalten.

Bei Penetrationstests werden im Gegensatz zu den üblichen funktionalen Tests die für erfolgreiche Cyberangriffe relevanten Eigenschaften getestet. Dabei handelt es sich z. B. um Negativtests oder Sicherheitseigenschaften, wie die Stärke von Sicherheitsfunktionen und die Entropie des verwendeten kryptografischen Schlüsselmaterials. Bislang fanden solche Tests oft erst in den fortgeschrittenen Entwicklungsphasen statt und verlangen neben spezieller Expertise auch einen hohen manuellen Arbeitsaufwand.

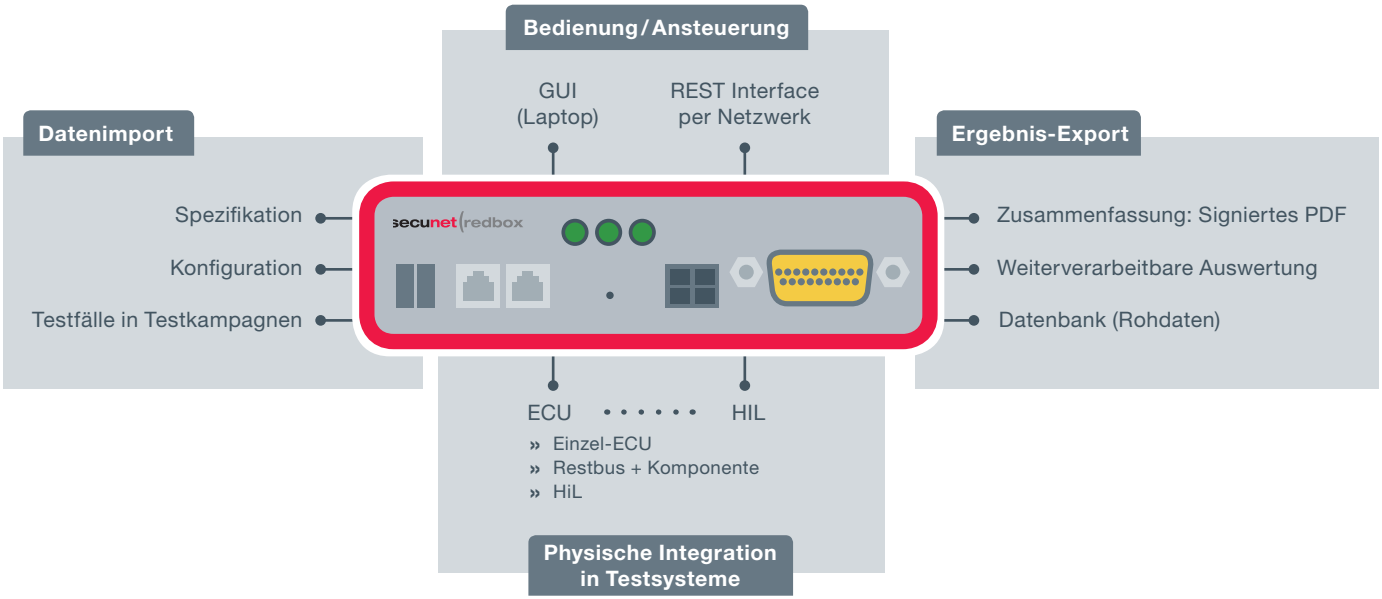
secunet redbox – Security effizient testen

Mit der redbox liefert secunet eine integrierte und flexible Lösung zur automatisierten Durchführung entwicklungsbegleitender Security-Tests. Sie basiert auf umfassenden und in einer Vielzahl von Penetrationstests bereits bewährten Werkzeugen und ermöglicht neben dem Effizienzgewinn durch Automatisierung auch eine bessere Testabdeckung und Dokumentation für einheitliche und vergleichbare Ergebnisse.

Auf Basis vorher definierter Testfälle können komplexe Kampagnen erstellt werden. Damit können auch aufwendige Untersuchungen mit nur einem Klick gestartet und jederzeit wiederholt werden. Alle durchgeführten Analysen und deren Ergebnisse werden automatisch dokumentiert und sicher archiviert.

Die redbox ist nicht nur für den Test einzelner Steuergeräte oder Komponenten gedacht, sondern kann auch eingesetzt werden, um einen Komponenten-Verbund oder Teilsysteme zu testen. Auch der Einsatz an Testarbeitsplätzen für funktionale Abnahmetests oder in Hardware-in-the-Loop (HiL) Systemen ist möglich.

Integrierte Lösung für effizientes Security Testing

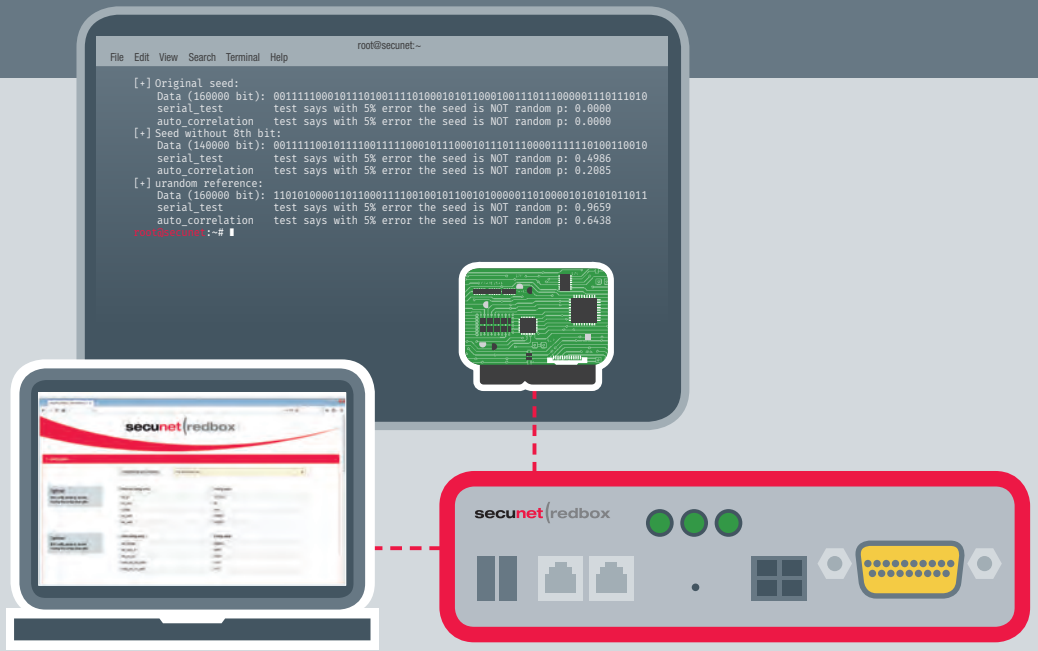


Von Pentestern – für Entwickler von Steuergeräten

Durch den Einsatz der redbox können große Teile der Reconnaissance-Phase von Penetrationstests automatisiert und verwaltet werden. Die Ergebnisse werden verschlüsselt und zugriffsgeschützt im System (innerhalb der secunet redbox) oder auf einem Netzwerkshare abgelegt.

Ist das System einmal konfiguriert und eingerichtet, lassen sich die definierten Basis-Penetrationstests auch von Mitarbeitern ohne spezielles Security-Know-how problemlos starten und durchführen. Security-Tests, u. a. Fuzzing, werden automatisiert, wodurch interne oder externe Experten für Penetrationstests sich verstärkt auf komplexe, manuelle Angriffe konzentrieren können.

Darüber hinaus ist sichergestellt, dass im Fehlerfall die Tests umfassend analysiert und bei Bedarf identisch wiederholt werden können. Damit bietet die redbox die optimale Unterstützung, um grundlegende Sicherheitsaspekte frühzeitig und regelmäßig in der Entwicklung von Steuergeräten abzusichern.



Produktmerkmale – Ihre Vorteile auf einen Blick

Mehrwerte

- Freie Ressourcen durch Automatisierung
- Die Bedienung erfordert kein spezielles Pentest- oder Security-Know-How
- Testkataloge für: Fuzzing / Undocumented Interfaces / UDS Scanning / Security Access
- Möglichkeit zur eigenen Entwicklung spezifischer Testfälle
- Geringerer Ressourcenbedarf für Basis-Security-Tests
- Langfristig belastbare Roadmap und Unterstützung etablierter Datenformate und Standards

Vergleichbarkeit und Wiederholbarkeit

- Archivierung von Testszenarien und Testergebnissen
- Unterstützung von Regressions-tests
- Tests werden durch automa-tisierte Dokumentationen standardisiert beschrieben und vergleichbar

Security und Datenschutz

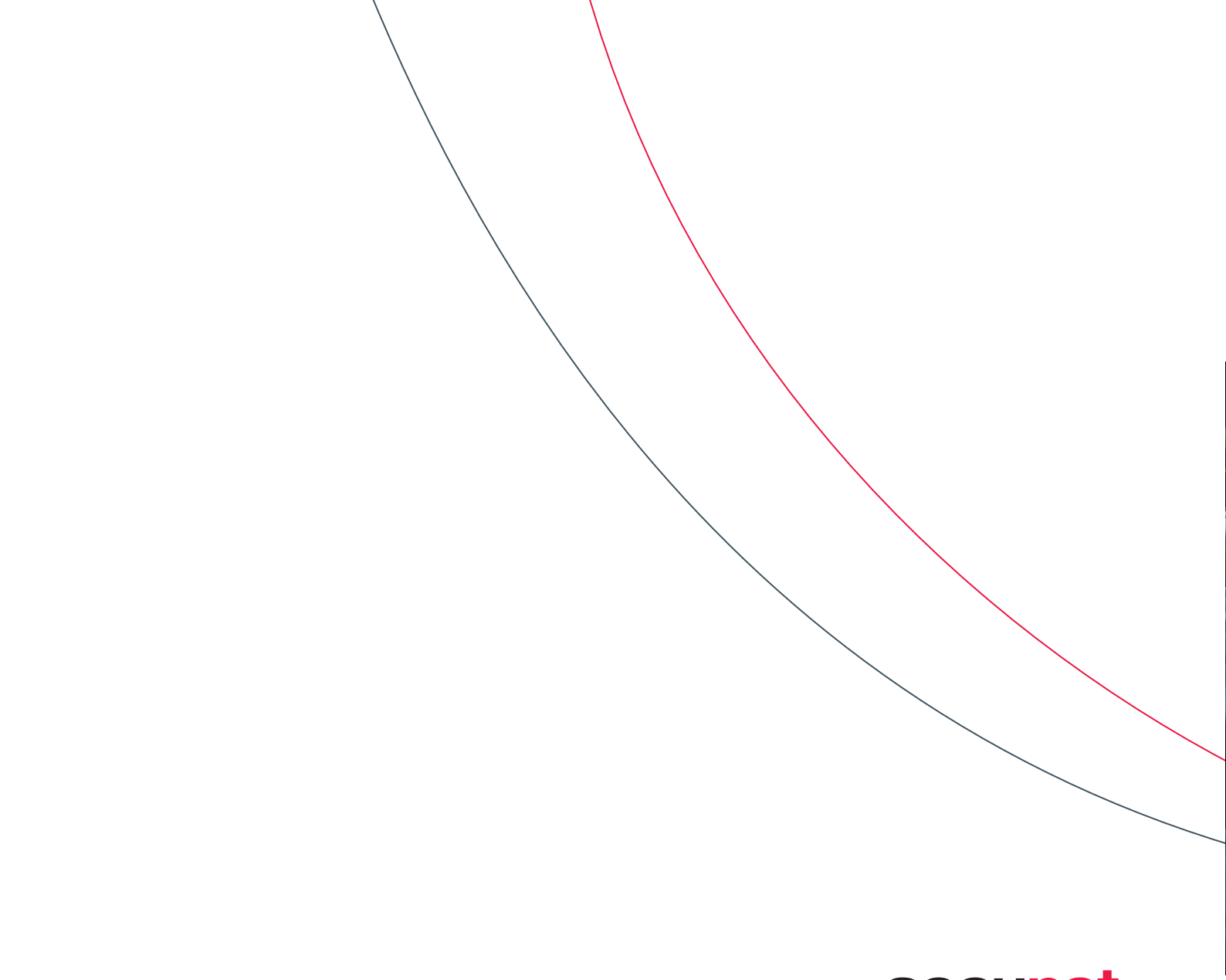
- Rollen- und Rechtekonzept erlaubt Steuerung von Zugriffen auf Testergebnisse
- Datenschutzkonforme Adminis-tration & verschlüsselte Ablage von sensitiven Daten

Technische Daten

- Scanning und Fuzzing von Netzwerk Protokollen
- Zustandsüberwachung der Prüflinge
- Busse: CAN-A / -B / -FD, Ethernet
- Protokolle: UDS, DoIP, ISO15765-2 (ISO-TP)
- Durchführung von automatischen Hard Resets der Prüflinge
- verschlüsselte Ablage von sensitiven Daten
- Erweiterbarkeit der Testumfänge in Phyton 3

Anwendergruppen

- Pentester / -innen
- ECU Verantwortliche
- Security Verantwortliche
- Test Verantwortliche



secunet

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

www.secunet.com