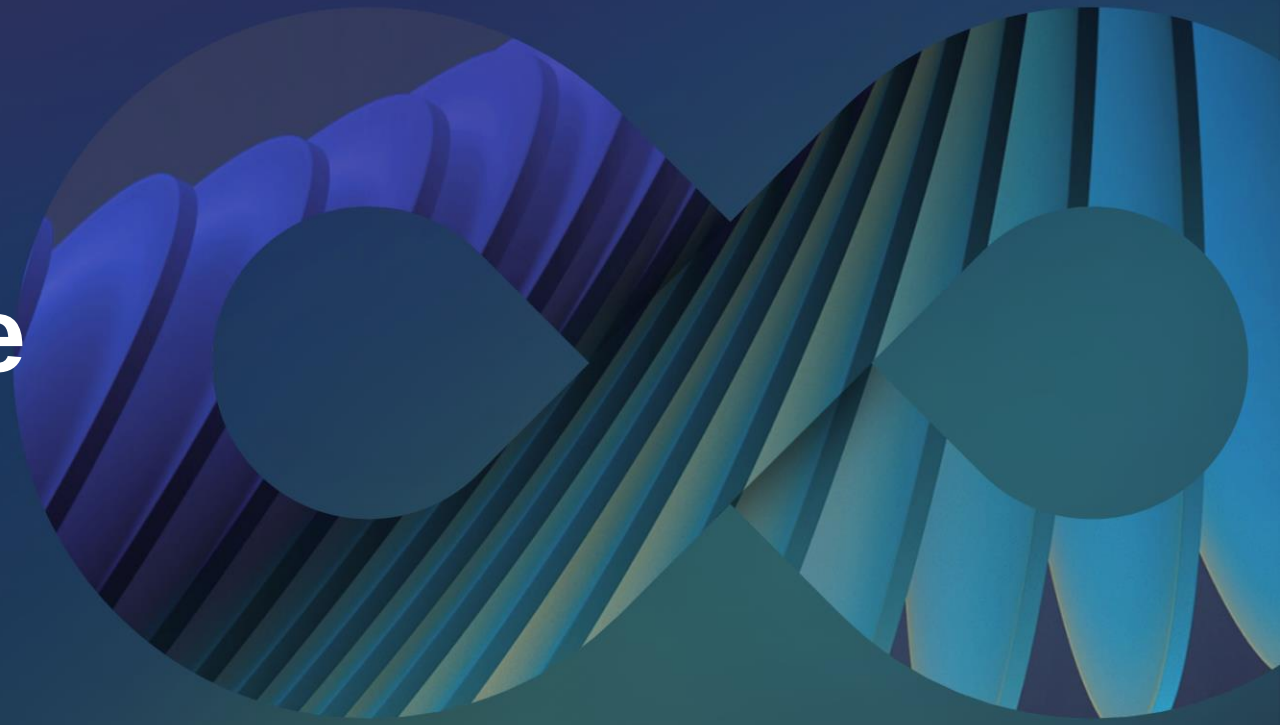
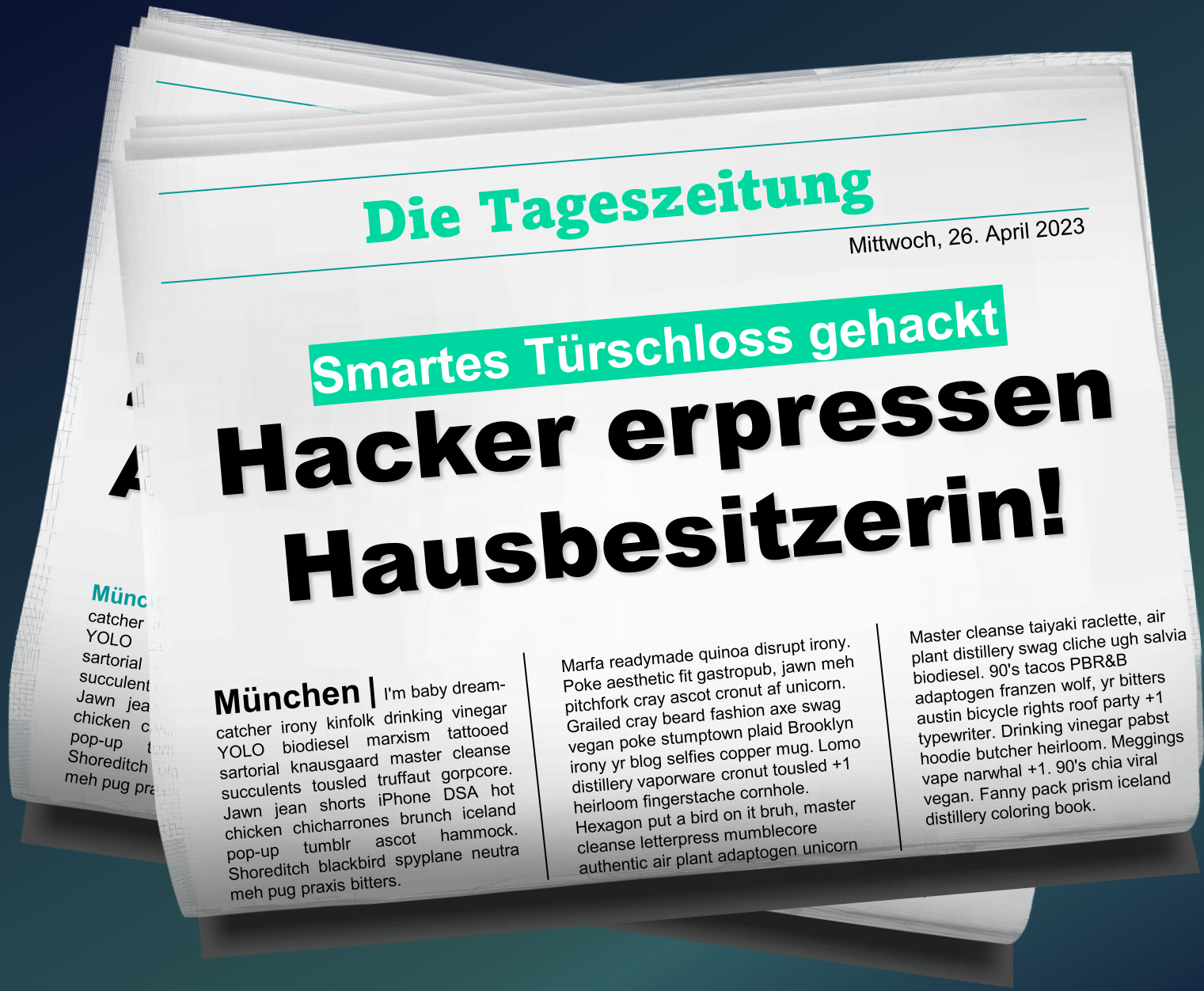
Warum sollte ich mir Gedanken machen, wenn meine Zahnbürste mit mir spricht?



Alexander Heyers
Siemens Digital Industries Software

SIEMENS

SIEMENS



SIEMENS

heise online heise+ Jetzt 1 Monat gratis testen

Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN:

KÜNSTLICHE INTELLIGENZ ENERGIE ELEKTROMOBILITÄT E-HEALTH WINDOWS LINUX & OPEN SOURCE PODCASTS

heise online > Google Pixel > Google Pixel: Exploit erlaubt Wiederherstellen nachträglich geänderter Bilder

Google Pixel: Exploit erlaubt Wiederherstellen nachträglich geänderter Bilder

Mit Googles Bildbearbeitung zugeschnittene Pixel-Screenshots können per "Acropalypse" reproduziert werden und sensible Daten verraten. Ein Patch ist verfügbar.

Lesezeit: 3 Min. In Pocket speichern 26

(Bild: quietbits/Shutterstock.com)

20.03.2023 03:08 Uhr | Security

Von Frank Schräer

Eine Sicherheitslücke in der Bildbearbeitung von Googles Pixel-Smartphones ermöglicht, dass nachträglich geänderte Screenshots zum großen Teil wiederhergestellt werden können. Dadurch könnten sensible Daten wie Adressen oder Zahlungsinformationen, die aus den Bildern herausgeschnitten oder übermalt wurden, reproduziert werden. Die Schwachstelle wurde mittlerweile von Google behoben, aber zuvor bereits verbreitete Bilder enthalten die Originalinforationen weiterhin.

Nach Angaben der Entdecker der Sicherheitslücke wurde diese bereits mit Android 9 (Pie) 2018 eingeführt. Seitdem überschreibt Google zwar nachträglich geänderte Screenshots auf Pixel-Smartphones über die Originaldatei, aber behält diese bei, wenn die neue Version kleiner ist als das Original. Das ist etwa dann der Fall, wenn eine Kreditkartennummer oder andere persönliche Informationen

UNSERE EMPFEHLUNG

Ratgeber

Sicherheits-Checkliste für Google

Für viele Nutzer steht der Google-Account im Zentrum aller Online-Aktivitäten. Wird er gekapert, drohen große Gefahren. So schützen Sie Ihr Konto.

heise+ 1 c't Magazin

SIEMENS

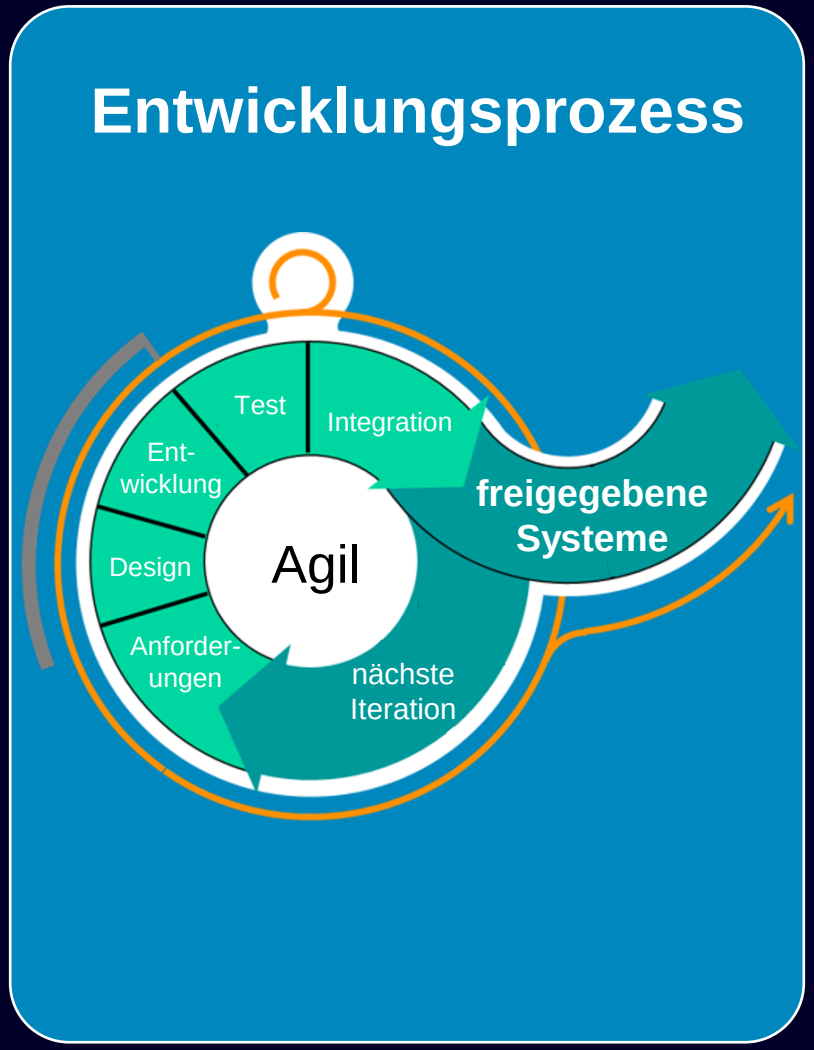

Unempfindlich gegen
Angriffe
Jederzeit sicher
Respektiert die
Privatsphäre
GO THE EXTRA
MILE

Produktentwicklung

Beispiel

SIEMENS

Produktentwicklung
Beispiel



SIEMENS

Werkzeuge
Spezialisten

Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit

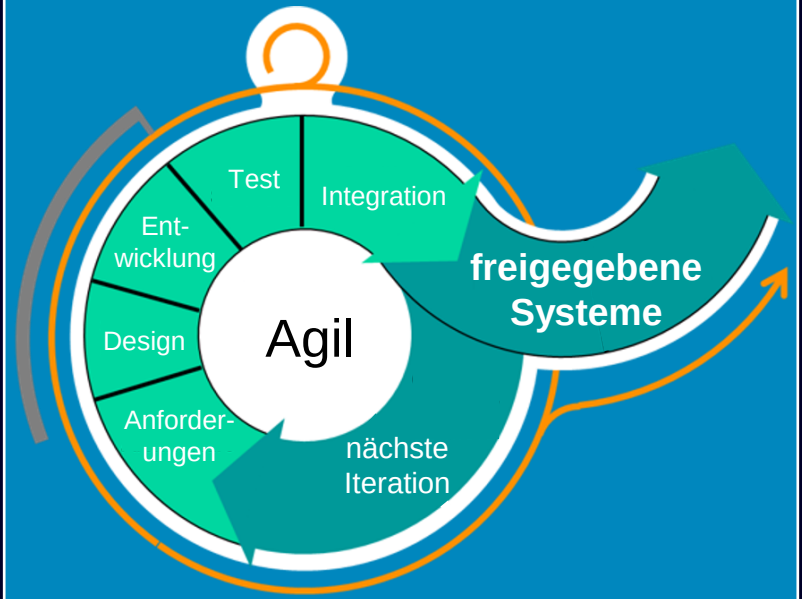
Analysewerkzeuge für Schaden, Gefährdung und Bedrohungszenarien

Risikobewertungen

Validierung

Berichte

Entwicklungsprozess



SIEMENS

Grenzen durchbrechen

Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit

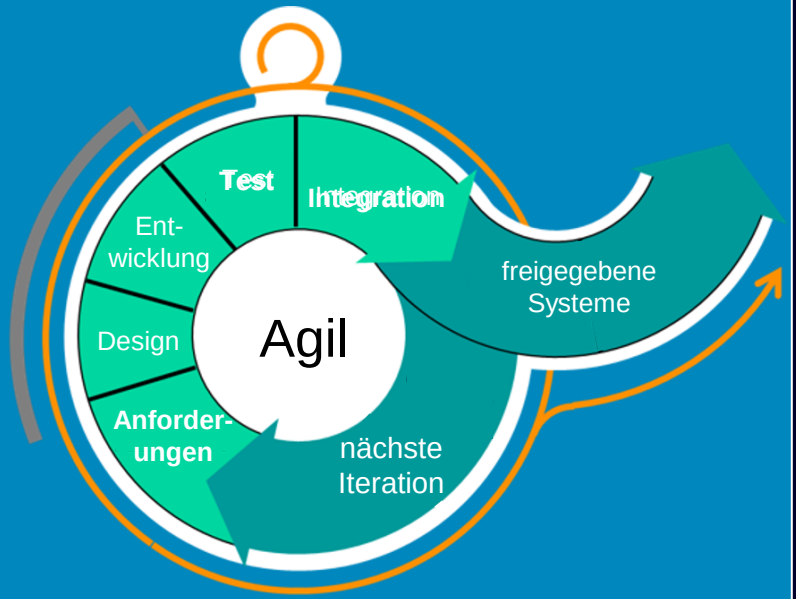
Analysewerkzeuge für Schaden, Gefährdung und Bedrohungszenarien

Risikobewertungen

Validierung

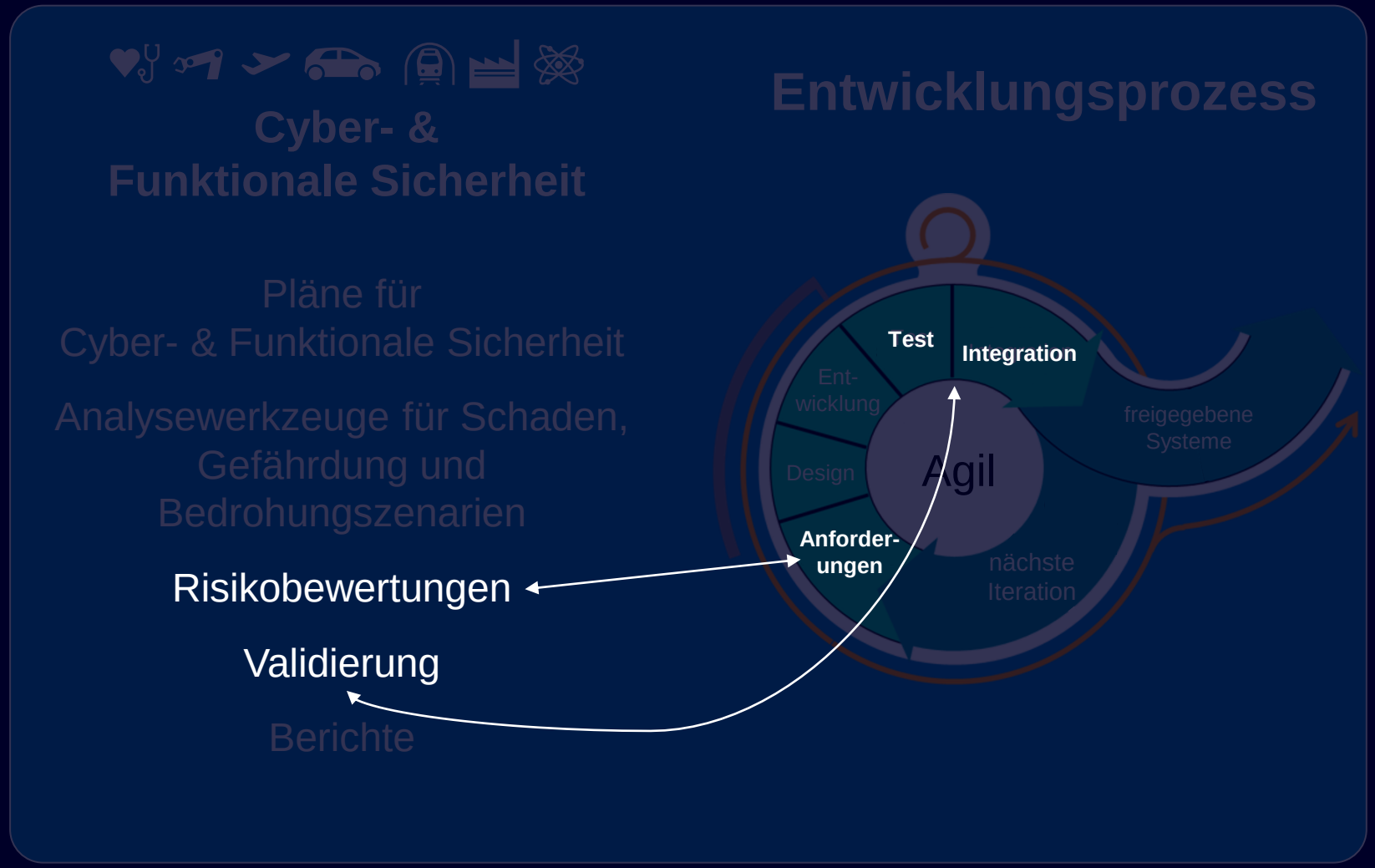
Berichte

Entwicklungsprozess



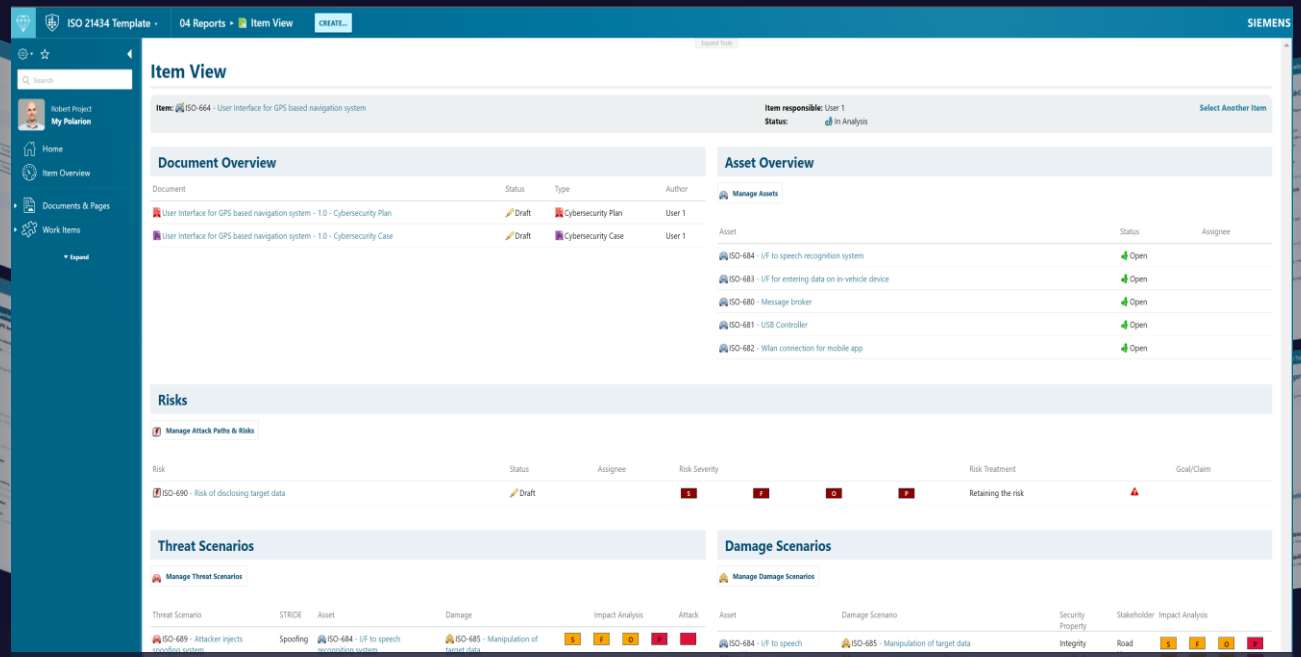
SIEMENS

Grenzen durchbrechen



SIEMENS

Direktes Zusammenspiel mit Polarion



Management Systeme
Durchgängiger Austausch von Informationen in die Entwicklung

Entscheidungshilfen
Bewertung von Sicherheitskontrollen und Abhilfemaßnahmen

Risiko-Bewertungen
Direkter Überblick über identifizierte Bedrohungen und Implikationen

SIEMENS

heise online

Jetzt 1 Monat gratis testen

Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN:

KÜNSTLICHE INTELLIGENZ ENERGIE ELEKTROMOBILITÄT E-HEALTH WINDOWS

LINUX & OPEN SOURCE PODCASTS

heise online > Google Pixel > Google Pixel: Exploit erlaubt Wiederherstellen nachträglich geänderter Bilder

Google Pixel: Exploit erlaubt Wiederherstellen nachträglich geänderter Bilder

Mit Googles Bildbearbeitung zugeschnittene Pixel-Screenshots können per "Acropalypse" reproduziert werden und sensible Daten verraten. Ein Patch ist verfügbar.

Lesezeit: 3 Min. In Pocket speichern 26

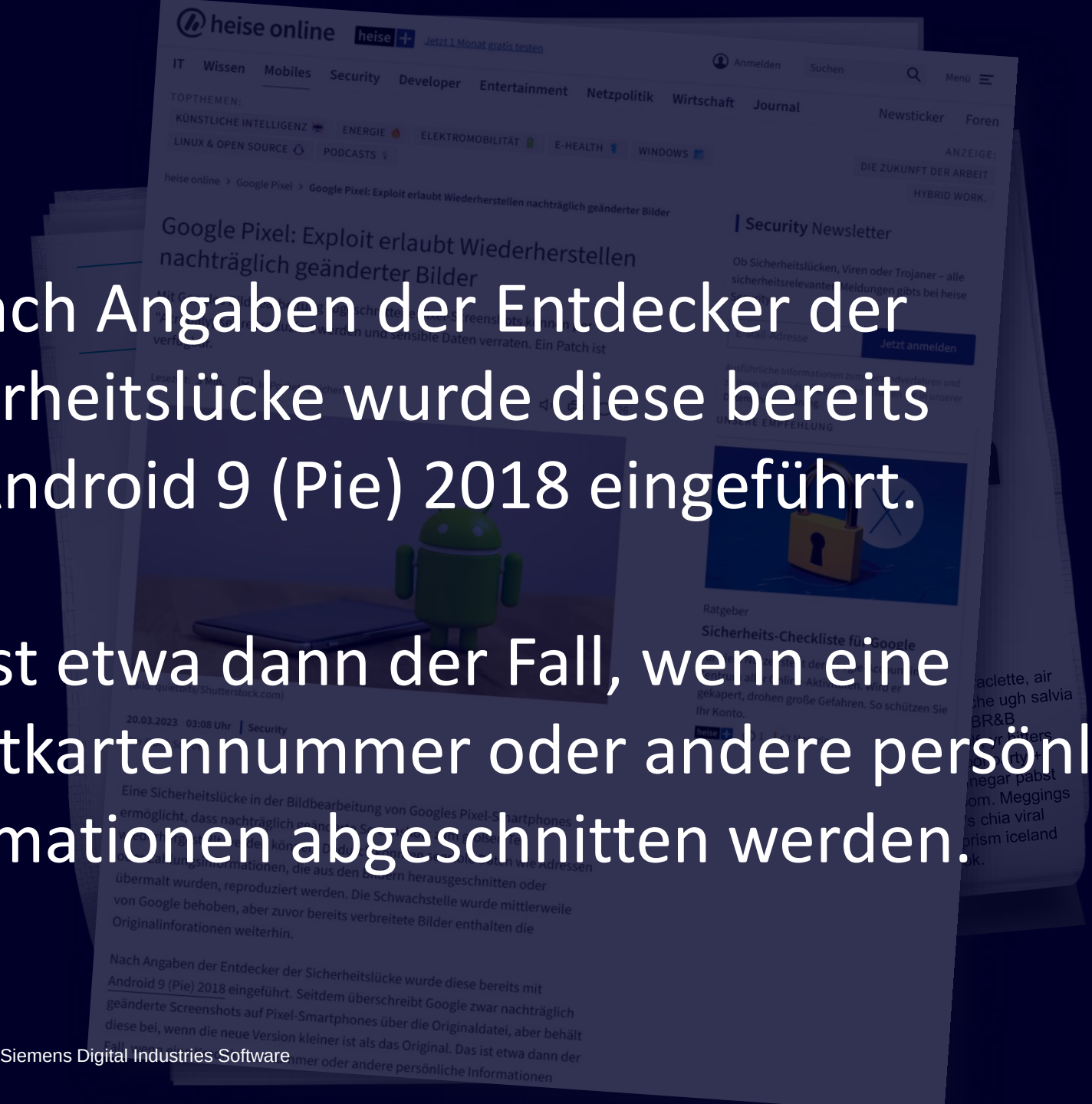
(Bild: quietbits/Shutterstock.com)

20.03.2023 03:08 Uhr | Security

Von Frank Schräer

Eine Sicherheitslücke in der Bildbearbeitung von Googles Pixel-Smartphones ermöglicht, dass nachträglich geänderte Screenshots zum großen Teil wiederhergestellt werden können. Dadurch könnten sensible Daten wie Adressen oder Zahlungsinformationen, die aus den Bildern herausgeschnitten oder übermalt wurden, reproduziert werden. Die Schwachstelle wurde mittlerweile von Google behoben, aber zuvor bereits verbreitete Bilder enthalten die Originalinforationen weiterhin.

Nach Angaben der Entdecker der Sicherheitslücke wurde diese bereits mit Android 9 (Pie) 2018 eingeführt. Seitdem überschreibt Google zwar nachträglich geänderte Screenshots auf Pixel-Smartphones über die Originaldatei, aber behält diese bei, wenn die neue Version kleiner ist als das Original. Das ist etwa dann der Fall, wenn eine Kreditkartennummer oder andere persönliche Informationen



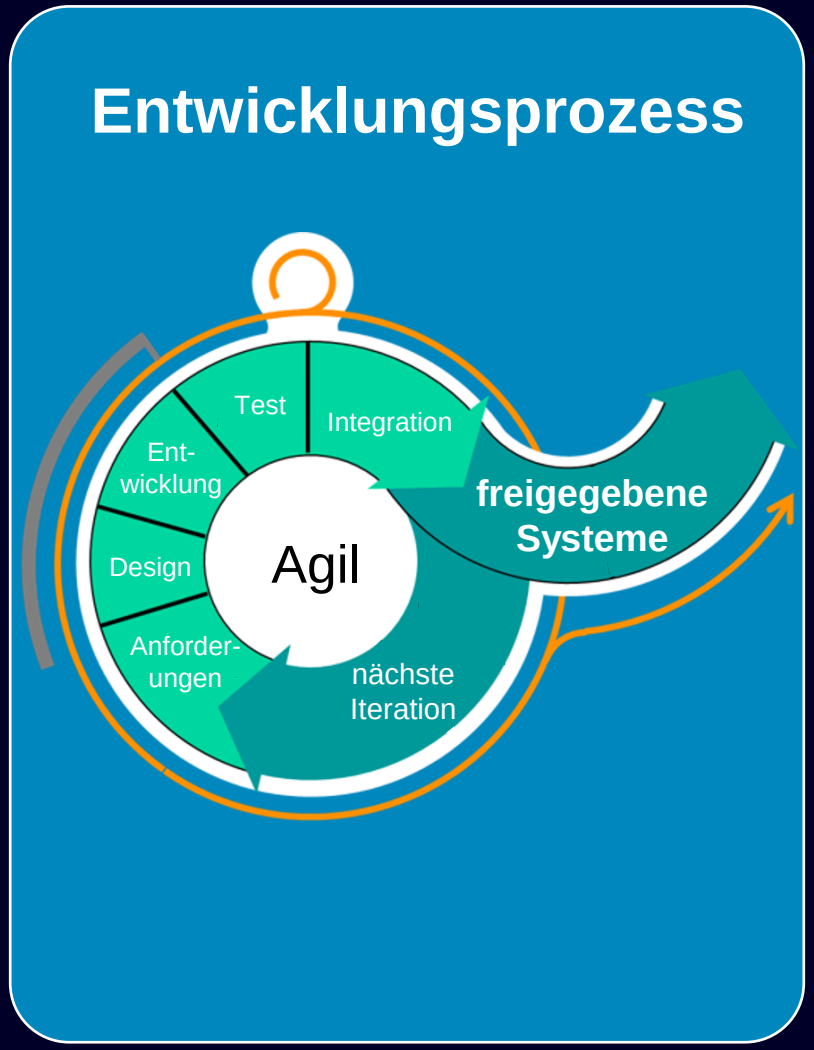
"Nach Angaben der Entdecker der Sicherheitslücke wurde diese bereits mit Android 9 (Pie) 2018 eingeführt.

...

Das ist etwa dann der Fall, wenn eine Kreditkartennummer oder andere persönliche Informationen abgeschnitten werden.

SIEMENS

Produktentwicklung
Beispiel



SIEMENS

Qualitätssicherung

Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit

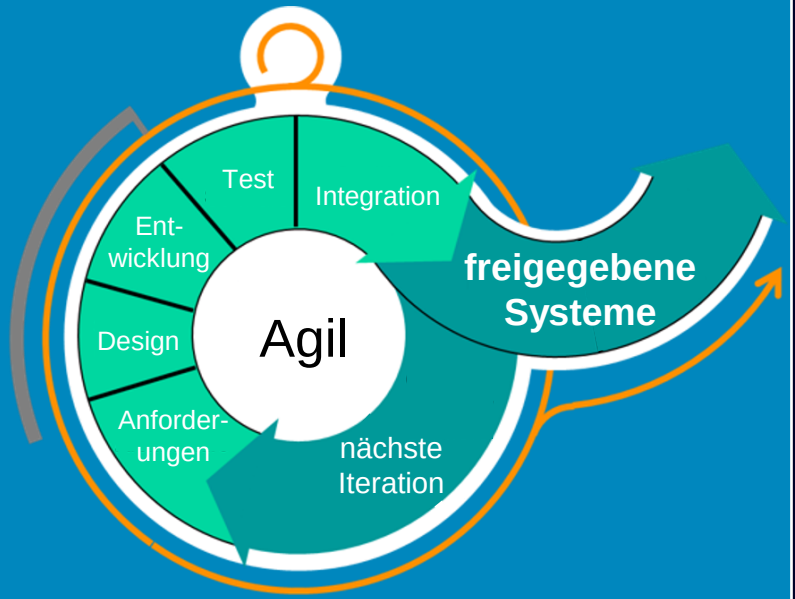
Analysewerkzeuge für Schaden, Gefährdung und Bedrohungszenarien

Risikobewertungen

Validierung

Berichte

Entwicklungsprozess



Qualitätsüberwachung

Sigrid

made by SIG

Code Qualität

Architekturanalyse

Open Source Überwachung

Risikobasierte Analysewerkzeuge

Trendberichte

SIEMENS

Kontinuerliche Qualitätssicherung

Cyber- & Funktionale Sicherheit

Pläne für Cyber- & Funktionale Sicherheit

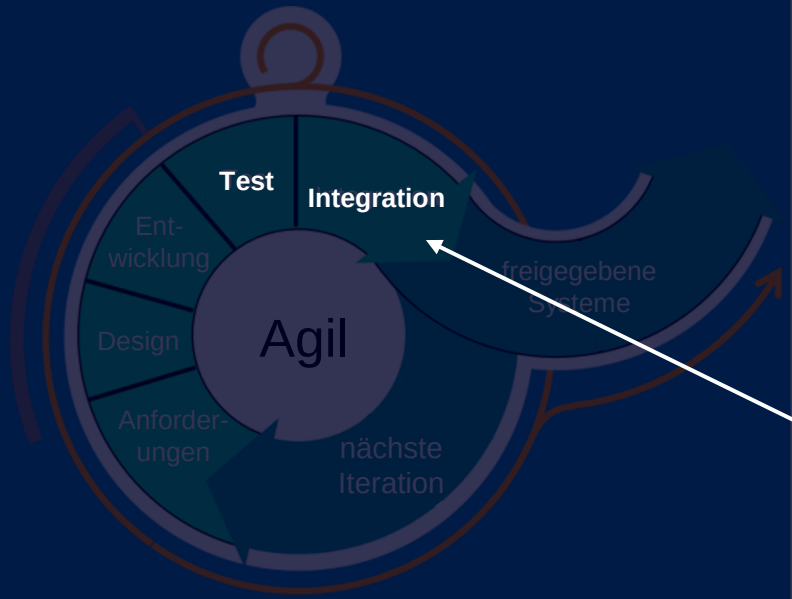
Analysewerkzeuge für Schaden, Gefährdung und Bedrohungszenarien

Risikobewertungen

Validierung

Berichte

Entwicklungsprozess



Qualitätsüberwachung

Sigrid

made by SIG

Code Qualität

Architekturanalyse

Open Source Überwachung

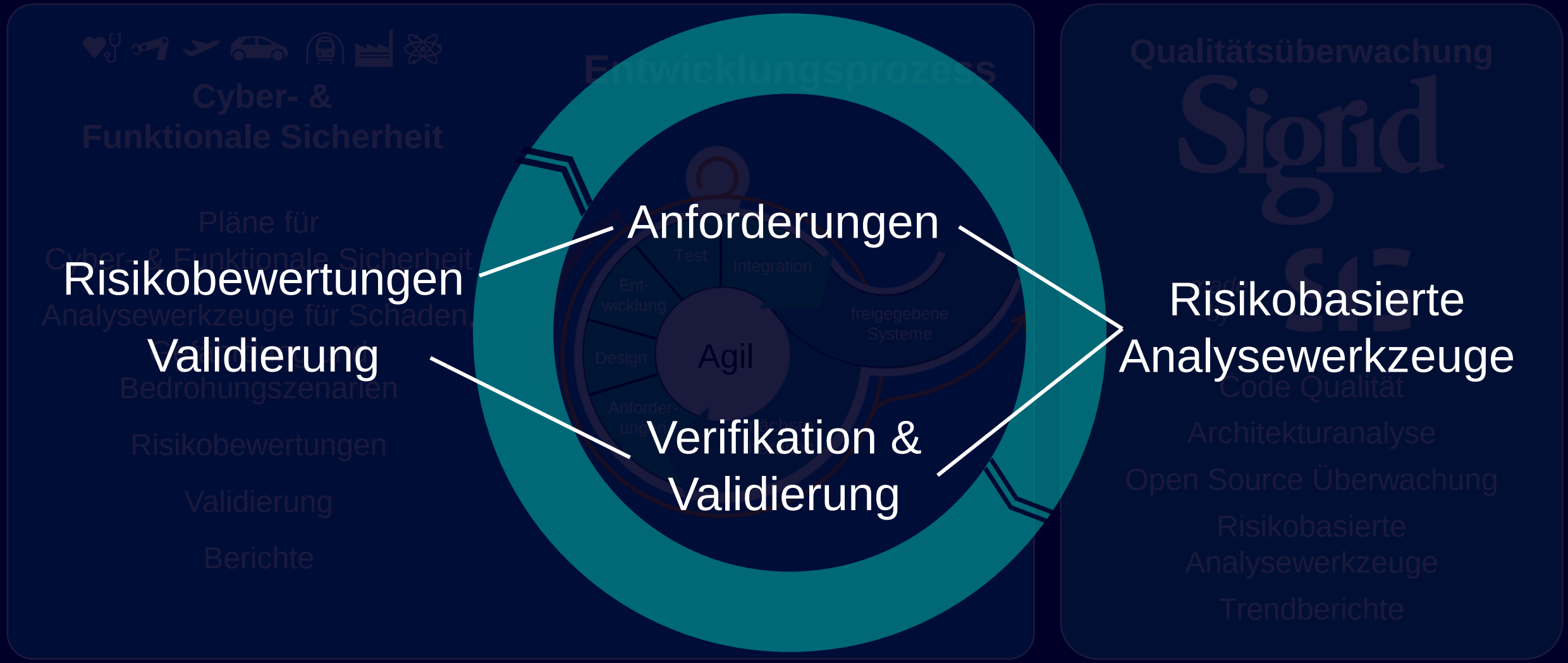
Risikobasierte Analysewerkzeuge

Trendberichte

SIEMENS

Ein Schritt weiter

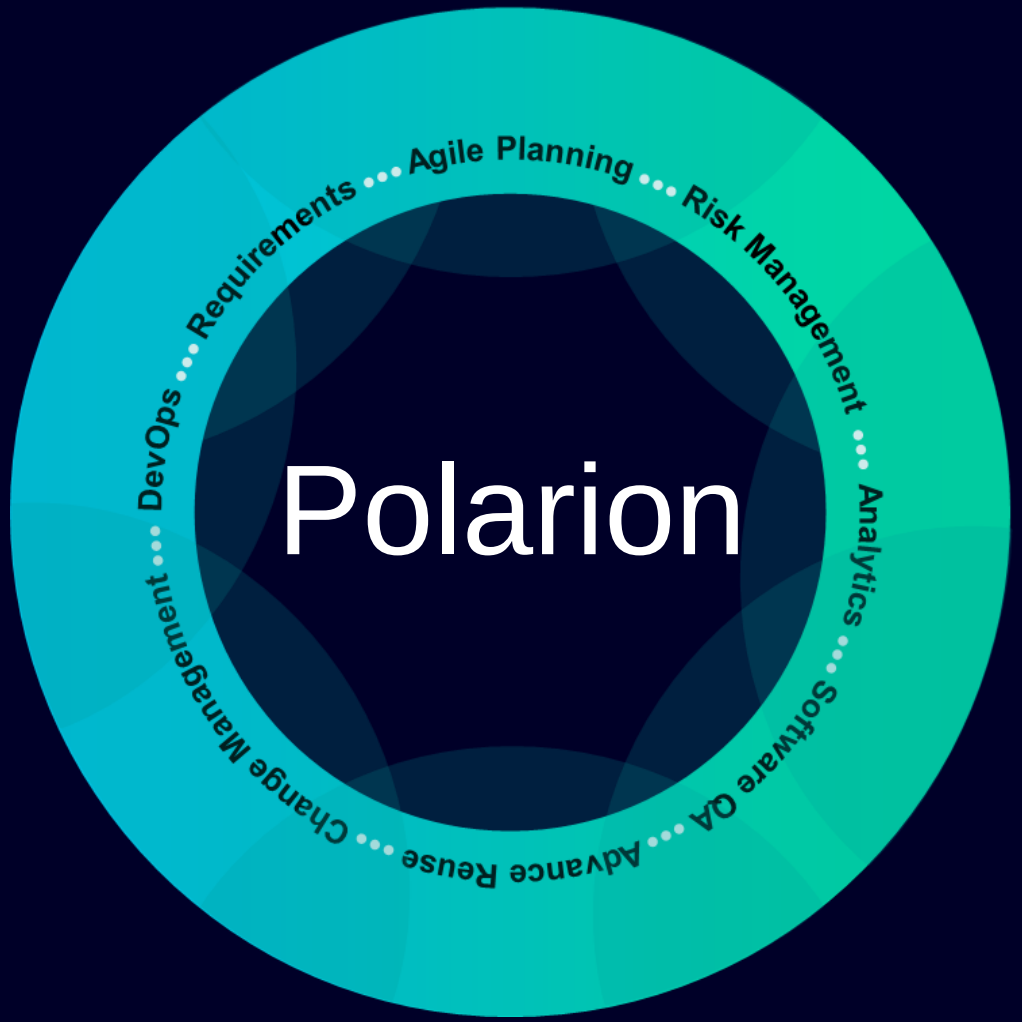
Automatischer Sicherheitslebenszyklus im Zusammenspiel



SIEMENS

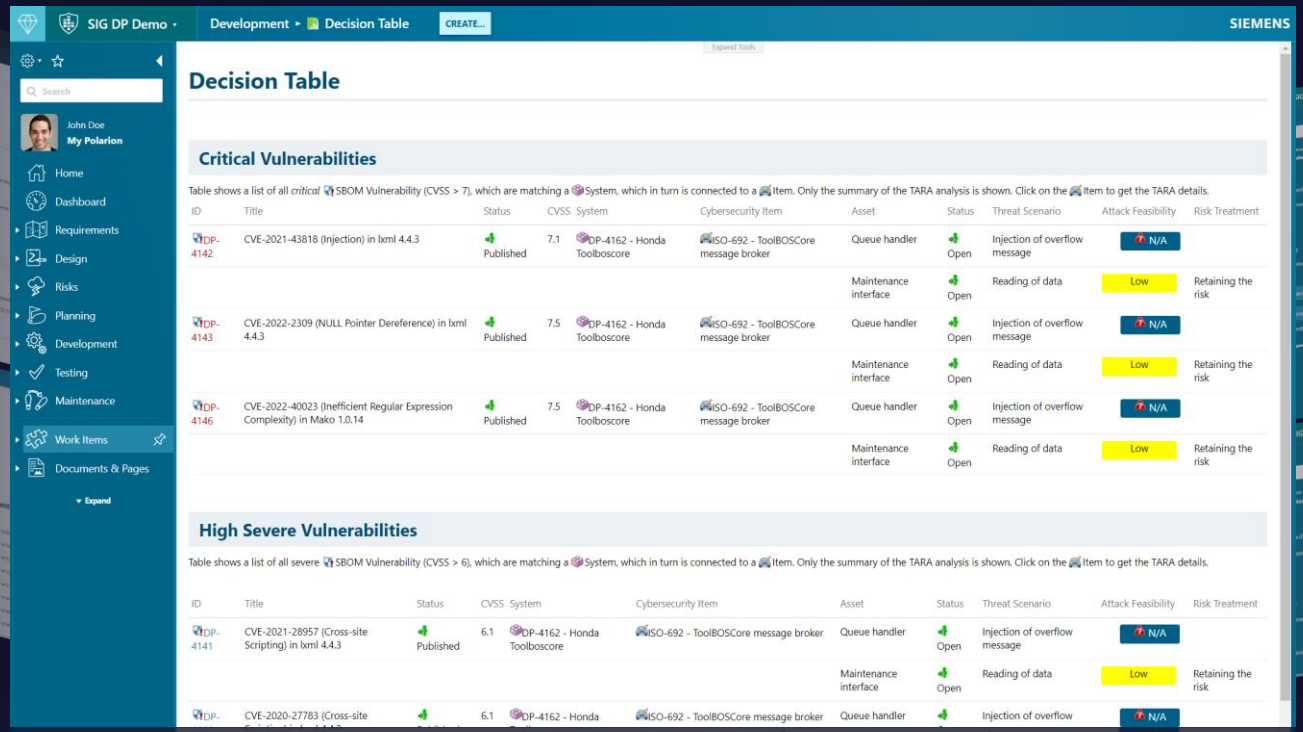
Ein Schritt weiter

Automatischer Sicherheitslebenszyklus im Zusammenspiel



Ein Schritt weiter

Automatischer Sicherheitslebenszyklus im Zusammenspiel



Qualitätsanalyse
Permanente Überwachung der gelieferten Software und Komponenten

Informationsaustausch
Bewertungen von Anforderungen, Tests und Risiken

SBOM – Software Bill of Material
Detaillierte Informationen zur Software Struktur

Vielen Dank für Ihre Aufmerksamkeit!

Alexander Heyers
Polarion PreSales Solution Consultant
Siemens Digital Industries Software

Mobile: +49 173 364 0020
E-mail: alexander.heyers@siemens.com