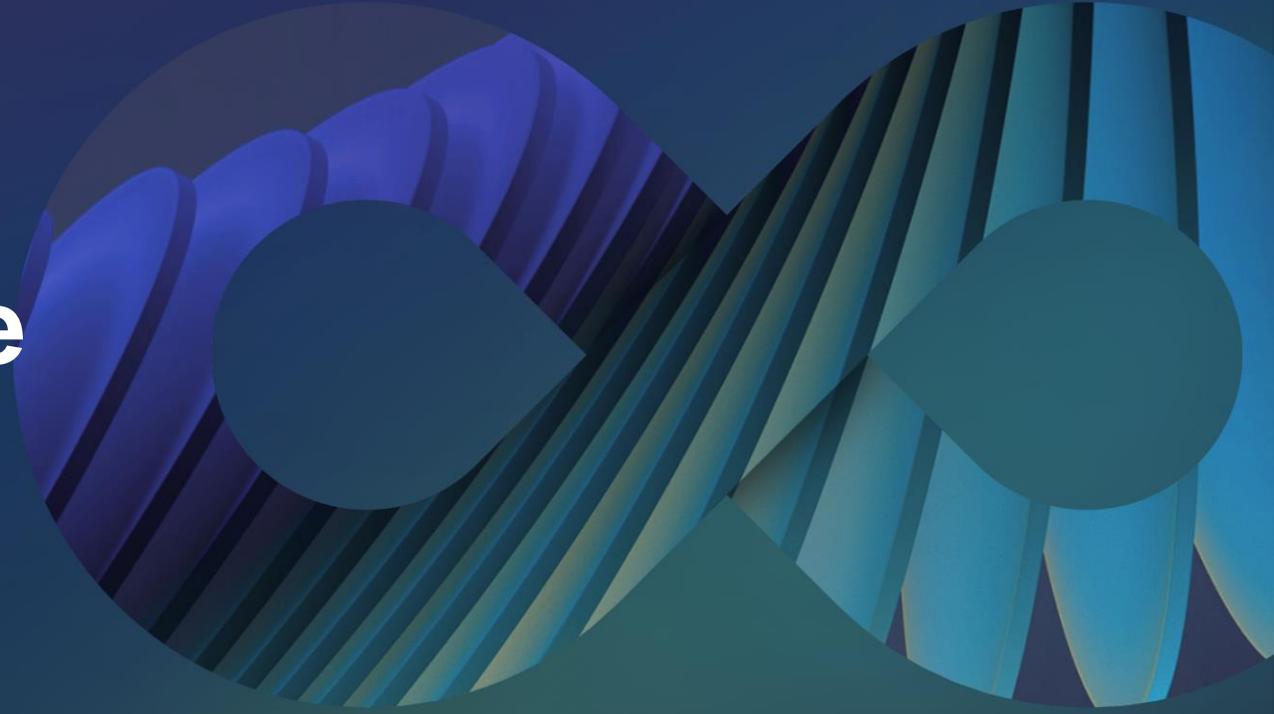


Warum sollte ich mir Gedanken machen, wenn meine Zahnbürste mit mir spricht?

Alexander Heyers

Siemens Digital Industries Software



Schlagzeilen der Welt

Mittwoch, 26. April 2023

Einbrecher räumen Wohnung leer!

Zahnbürste verwickelt Anwender in Gespräch



München | I'm baby dream-catcher irony kinfolk drinking vinegar YOLO biodiesel marxism tattooed sartorial knausgaard master cleanse succulents tousled truffaut gorpcore. Jawn jean shorts iPhone DSA hot chicken chicharrones brunch iceland pop-up tumblr ascot hammock. Shoreditch blackbird spyplane neutra meh pug praxis bitters.

Marfa readymade quinoa disrupt irony. Poke aesthetic fit gastropub, jawn meh pitchfork cray ascot cronut af unicorn. Grailed cray beard fashion axe swag vegan poke stumptown plaid Brooklyn irony yr blog selfies copper mug. Lomo distillery vaporware cronut tousled +1 heirloom fingerstache cornhole. Hexagon put a bird on it bruh, master cleanse letterpress mumblecore authentic air plant adaptogen unicorn

Master cleanse taiyaki raclette, air plant distillery swag cliché ugh salvia biodiesel. 90's tacos PBR&B adaptogen franzen wolf, yr bitters austin bicycle rights roof party +1 typewriter. Drinking vinegar pabst hoodie butcher heirloom. Meggings vape narwhal +1. 90's chia viral vegan. Fanny pack prism iceland distillery coloring book.

Die Tageszeitung

Mittwoch, 26. April 2023

Smartes Türschloss gehackt

Hacker erpressen Hausbesitzerin!

Münc
catcher
YOLO
sartorial
succulent
Jawn jea
chicken c
pop-up t
Shoreditch
meh pug pra

München | I'm baby dream-catcher irony kinfolk drinking vinegar YOLO biodiesel marxism tattooed sartorial knausgaard master cleanse succulents tousled truffaut gorpcore. Jawn jean shorts iPhone DSA hot chicken chicharrones brunch iceland pop-up tumblr ascot hammock. Shoreditch blackbird spyplane neutra meh pug praxis bitters.

Marfa readymade quinoa disrupt irony. Poke aesthetic fit gastropub, jawn meh pitchfork cray ascot cronut af unicorn. Grailed cray beard fashion axe swag vegan poke stumptown plaid Brooklyn irony yr blog selfies copper mug. Lomo distillery vaporware cronut tousled +1 heirloom fingerstache cornhole. Hexagon put a bird on it bruh, master cleanse letterpress mumblecore authentic air plant adaptogen unicorn

Master cleanse taiyaki raclette, air plant distillery swag cliché ugh salvia biodiesel. 90's tacos PBR&B adaptogen franzen wolf, yr bitters austin bicycle rights roof party +1 typewriter. Drinking vinegar pabst hoodie butcher heirloom. Meggings vape narwhal +1. 90's chia viral vegan. Fanny pack prism iceland distillery coloring book.

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

ANZEIGE: DIE ZUKUNFT DER ARBEIT HYBRID WORK.

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



(Bild: quietbits/Shutterstock.com)

20.03.2023 03:08 Uhr | Security
Von Frank Schröder

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 Originalinformationen 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

Security Newsletter

Ob Sicherheitslücken, Viren oder Trojaner - alle sicherheitsrelevanten Meldungen gibts bei heise Security

E-Mail-Adresse **Jetzt anmelden**

Ausführliche Informationen zum Versandverfahren und zu Ihren Widerrufsmöglichkeiten erhalten Sie in unserer Datenschutzerklärung.

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

Unempfindlich gegen
Angriffe

Jederzeit **sicher**

Respektiert die

Privatsphäre

GO THE EXTRA

MILE

Produktentwicklung

Beispiel



Produktentwicklung

Beispiel



Werkzeuge

Spezialisten



Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit

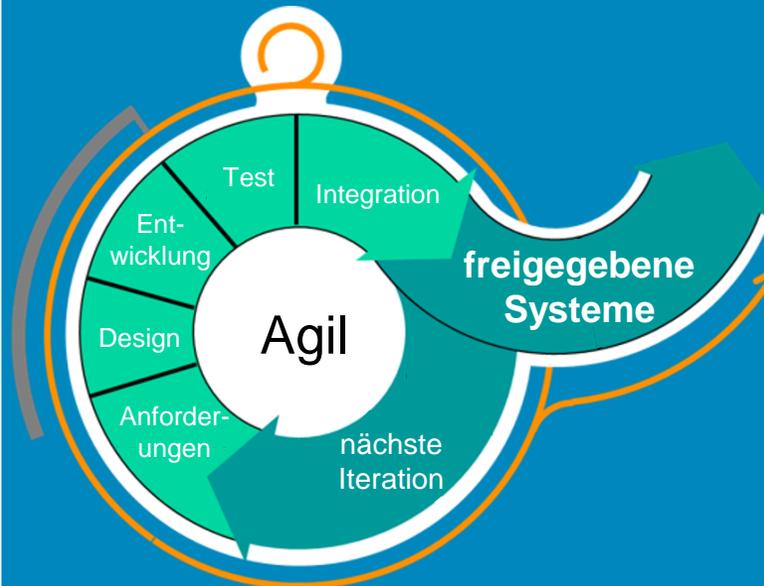
Analysewerkzeuge für Schaden,
Gefährdung und
Bedrohungsszenarien

Risikobewertungen

Validierung

Berichte

Entwicklungsprozess



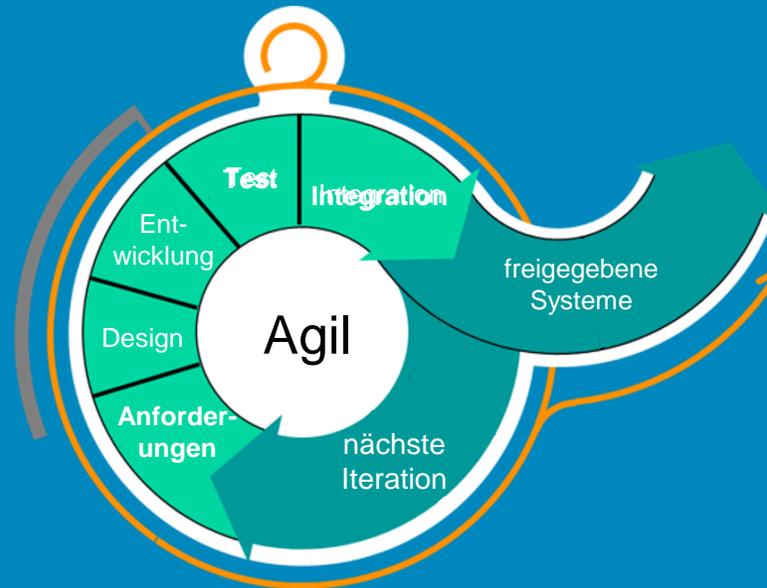
Grenzen durchbrechen



Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit
Analysewerkzeuge für Schaden,
Gefährdung und
Bedrohungsszenarien
Risikobewertungen
Validierung
Berichte

Entwicklungsprozess



Grenzen durchbrechen



Cyber- & Funktionale Sicherheit

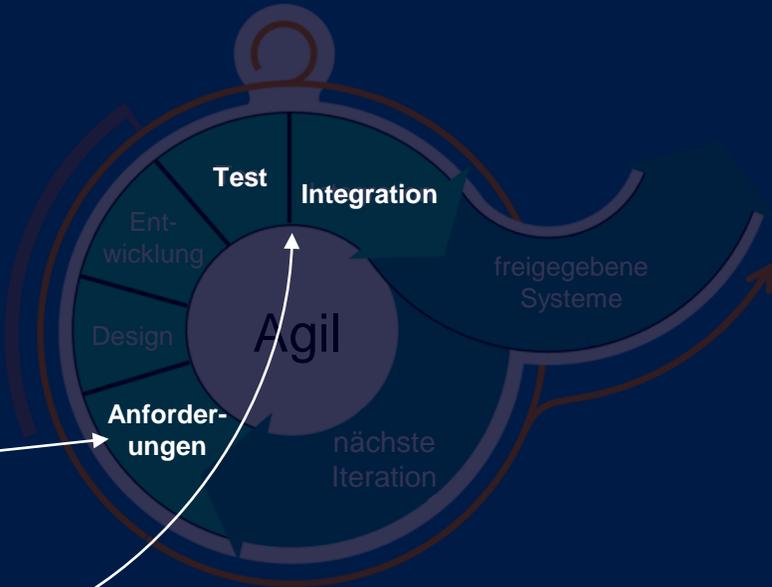
Pläne für Cyber- & Funktionale Sicherheit
Analysewerkzeuge für Schaden, Gefährdung und Bedrohungsszenarien

Risikobewertungen

Validierung

Berichte

Entwicklungsprozess



Direktes Zusammenspiel mit Polarion



Item View

Item: ISO-664 - User interface for GPS based navigation system

Item responsible: User 1

Status: In Analysis

Document Overview

Document	Status	Type	Author
User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan	Draft	Cybersecurity Plan	User 1
User Interface for GPS based navigation system - 1.0 - Cybersecurity Case	Draft	Cybersecurity Case	User 1

Asset Overview

Asset	Status	Assignee
ISO-684 - I/F to speech recognition system	Open	
ISO-683 - I/F for entering data on in-vehicle device	Open	
ISO-680 - Message broker	Open	
ISO-681 - USB Controller	Open	
ISO-682 - Wifi connection for mobile app	Open	

Risks

Manage Attack Paths & Risks

Risk	Status	Assignee	Risk Severity	Risk Treatment	Goal/Claim
ISO-690 - Risk of disclosing target data	Draft		High	Retaining the risk	

Threat Scenarios

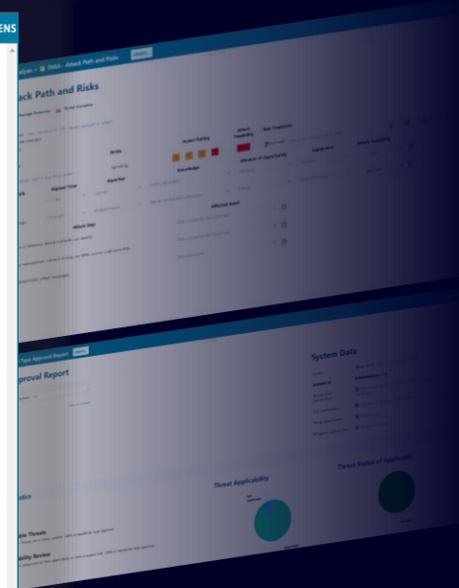
Manage Threat Scenarios

Threat Scenario	STRIDE	Asset	Damage	Impact Analysis	Attack
ISO-689 - Attacker injects malicious software	Spooling	ISO-684 - I/F to speech recognition system	ISO-685 - Manipulation of target data	High	High

Damage Scenarios

Manage Damage Scenarios

Asset	Damage Scenario	Security Property	Stakeholder	Impact Analysis
ISO-684 - I/F to speech	ISO-685 - Manipulation of target data	Integrity	Road	High



Management Systeme

Durchgängiger Austausch von Informationen in die Entwicklung



Entscheidungshilfen

Bewertung von Sicherheitskontrollen und Abhilfemaßnahmen



Risiko-Bewertungen

Direkter Überblick über identifizierte Bedrohungen und Implikationen

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

ANZEIGE: DIE ZUKUNFT DER ARBEIT HYBRID WORK.

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 Schröder

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 Originalinformationen 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

Security Newsletter

Ob Sicherheitslücken, Viren oder Trojaner - alle sicherheitsrelevanten Meldungen gibts bei heise Security

E-Mail-Adresse **Jetzt anmelden**

Ausführliche Informationen zum Versandverfahren und zu Ihren Widerrufsmöglichkeiten erhalten Sie in unserer Datenschutzerklärung.

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.

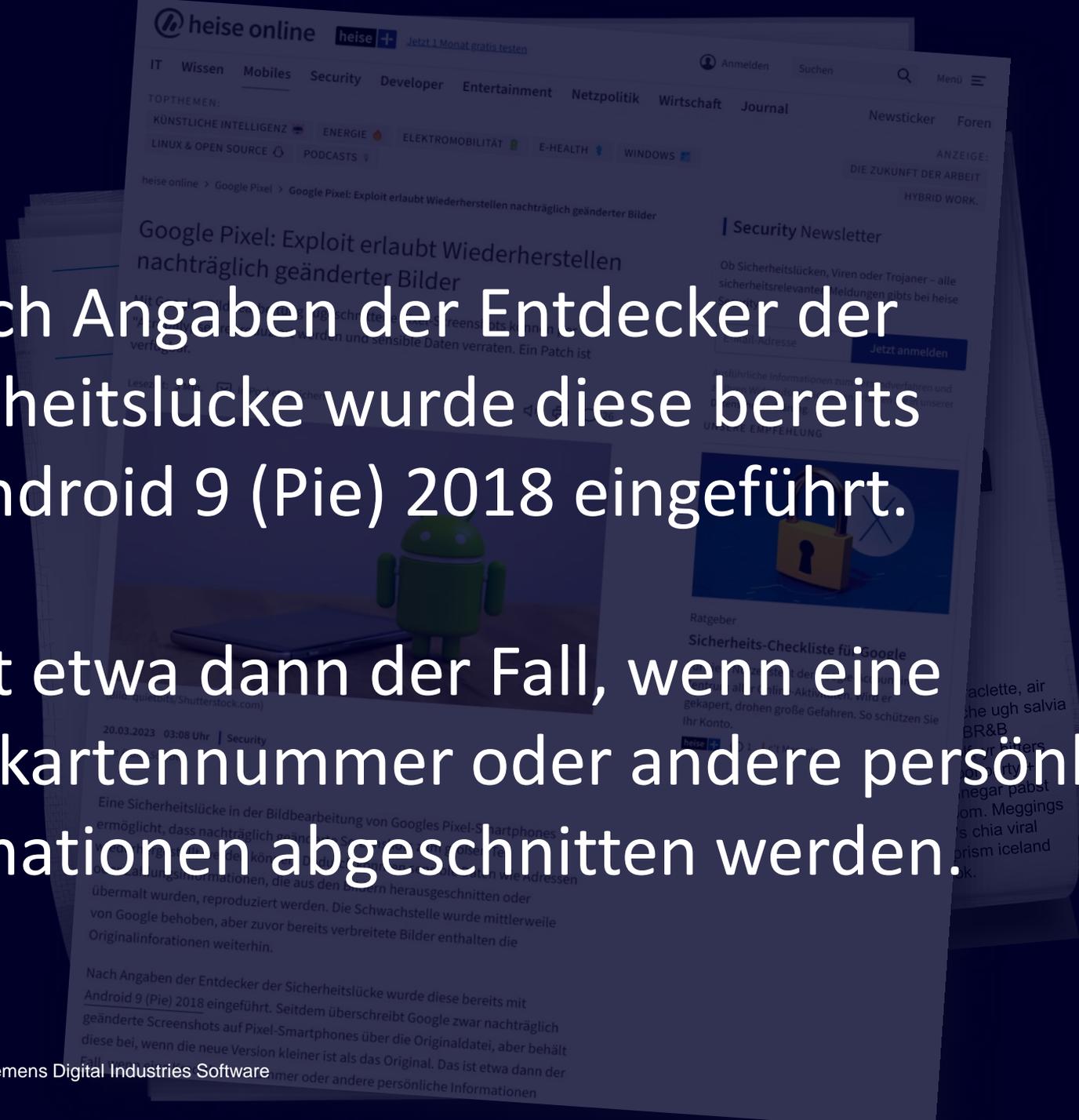
heise + 1 c't Magazin



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.



Produktentwicklung

Beispiel



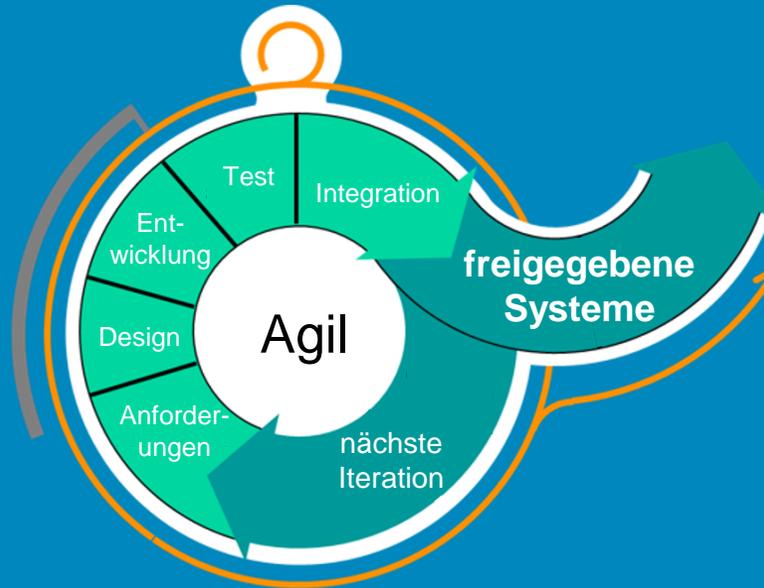
Qualitätssicherung



Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit
Analysewerkzeuge für Schaden,
Gefährdung und
Bedrohungsszenarien
Risikobewertungen
Validierung
Berichte

Entwicklungsprozess



Qualitätsüberwachung

Sigrid

made
by
SI

Code Qualität
Architekturanalyse
Open Source Überwachung
Risikobasierte
Analysewerkzeuge
Trendberichte

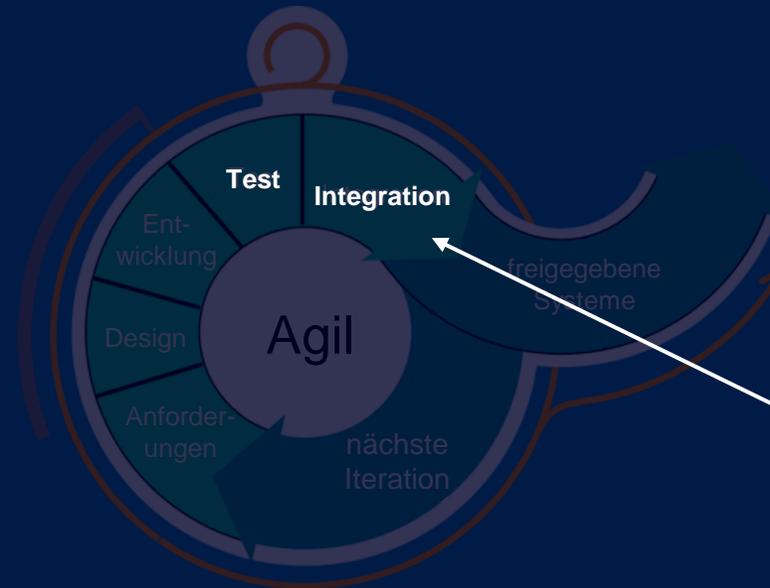
Kontinuierliche Qualitätssicherung



Cyber- & Funktionale Sicherheit

Pläne für
Cyber- & Funktionale Sicherheit
Analysewerkzeuge für Schaden,
Gefährdung und
Bedrohungsszenarien
Risikobewertungen
Validierung
Berichte

Entwicklungsprozess



Qualitätsüberwachung

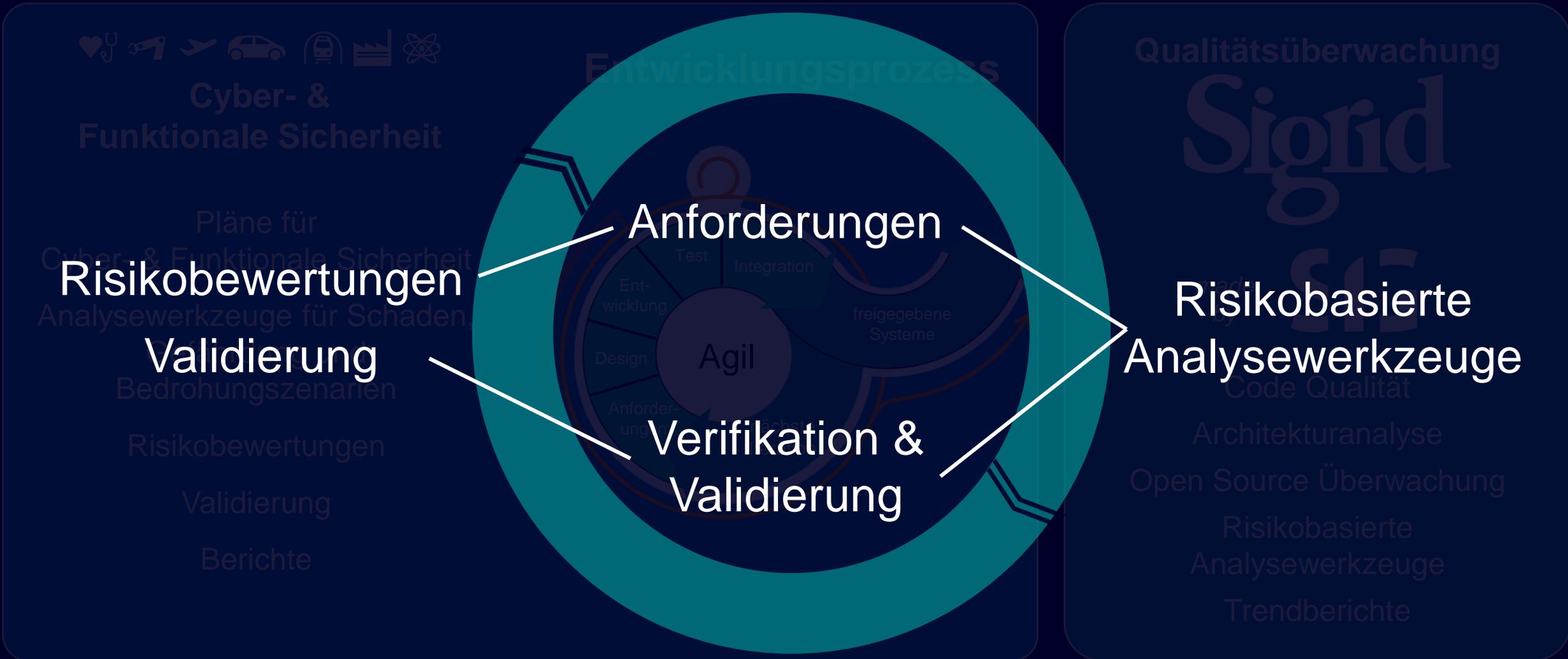
Sigrid

made
by
SIG

Code Qualität
Architekturanalyse
Open Source Überwachung
Risikobasierte
Analysewerkzeuge
Trendberichte

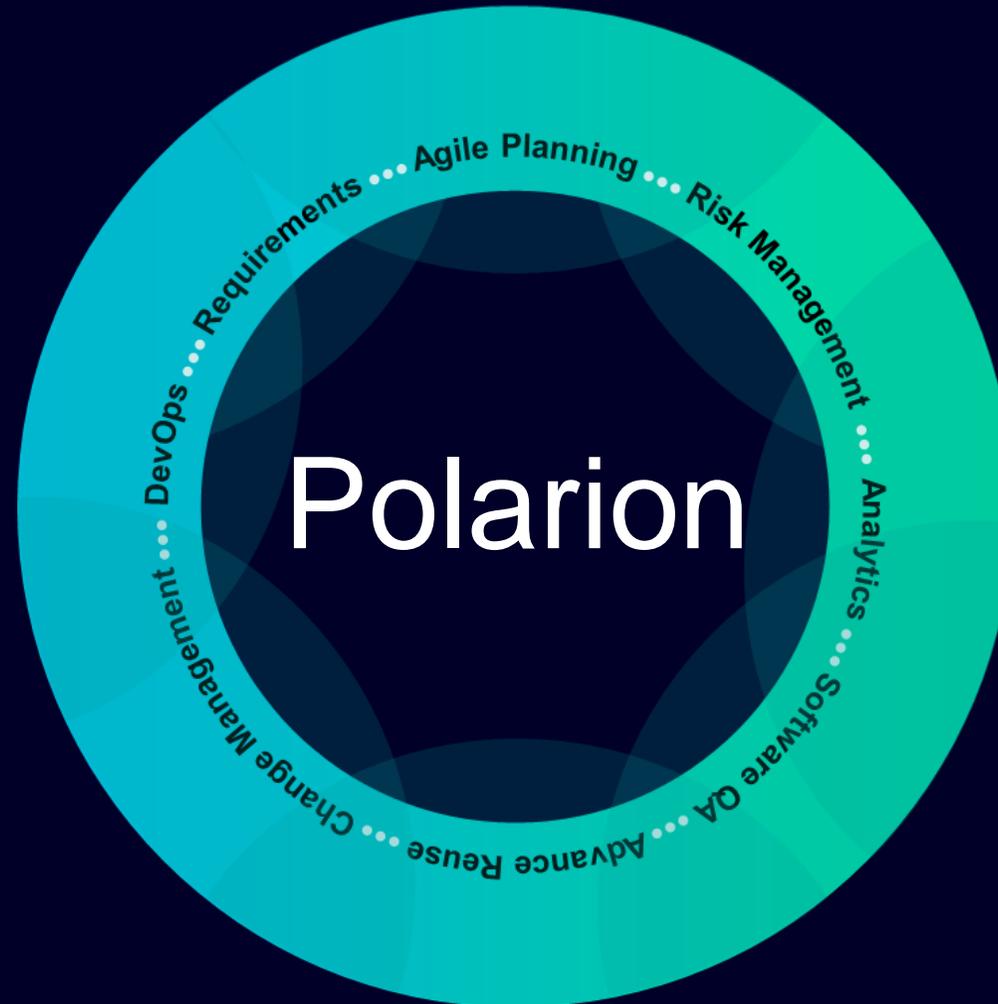
Ein Schritt weiter

Automatischer Sicherheitslebenszyklus im Zusammenspiel



Ein Schritt weiter

Automatischer Sicherheitslebenszyklus im Zusammenspiel



Ein Schritt weiter

Automatischer Sicherheitslebenszyklus im Zusammenspiel



Decision Table

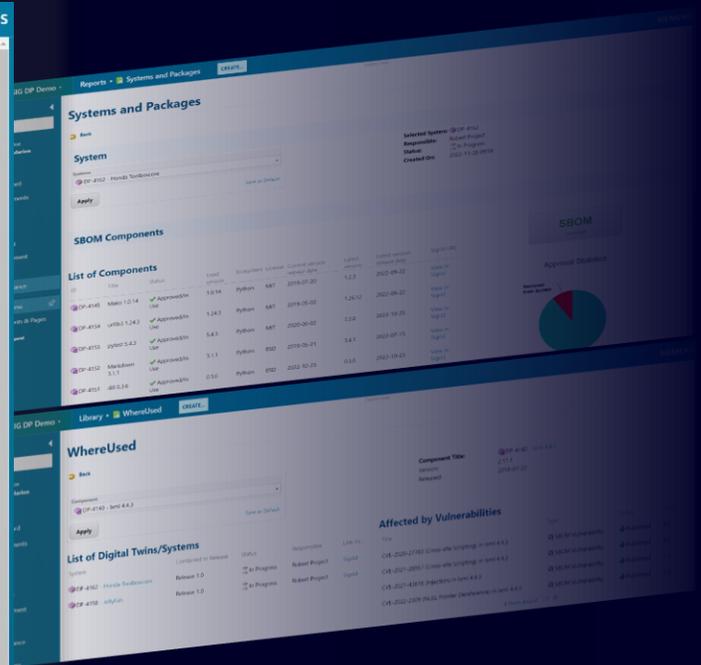
Table shows a list of all critical SBOM Vulnerability (CVSS > 7), which are matching a System, which in turn is connected to a Item. Only the summary of the TARA analysis is shown. Click on the Item to get the TARA details.

ID	Title	Status	CVSS	System	Cybersecurity Item	Asset	Status	Threat Scenario	Attack Feasibility	Risk Treatment
DP-4142	CVE-2021-43818 (injection) in kxml 4.4.3	Published	7.1	DP-4162 - Honda Toolboscore	ISO-692 - ToolBOSCore message broker	Queue handler	Open	Injection of overflow message	N/A	
						Maintenance interface	Open	Reading of data	Low	Retaining the risk
DP-4143	CVE-2022-2309 (NULL Pointer Dereference) in kxml 4.4.3	Published	7.5	DP-4162 - Honda Toolboscore	ISO-692 - ToolBOSCore message broker	Queue handler	Open	Injection of overflow message	N/A	
						Maintenance interface	Open	Reading of data	Low	Retaining the risk
DP-4146	CVE-2022-40023 (Inefficient Regular Expression Complexity) in Mako 1.0.14	Published	7.5	DP-4162 - Honda Toolboscore	ISO-692 - ToolBOSCore message broker	Queue handler	Open	Injection of overflow message	N/A	
						Maintenance interface	Open	Reading of data	Low	Retaining the risk

High Severe Vulnerabilities

Table shows a list of all severe SBOM Vulnerability (CVSS > 6), which are matching a System, which in turn is connected to a Item. Only the summary of the TARA analysis is shown. Click on the Item to get the TARA details.

ID	Title	Status	CVSS	System	Cybersecurity Item	Asset	Status	Threat Scenario	Attack Feasibility	Risk Treatment
DP-4141	CVE-2021-28957 (Cross-site Scripting) in kxml 4.4.3	Published	6.1	DP-4162 - Honda Toolboscore	ISO-692 - ToolBOSCore message broker	Queue handler	Open	Injection of overflow message	N/A	
						Maintenance interface	Open	Reading of data	Low	Retaining the risk
DP-	CVE-2020-27783 (Cross-site		6.1	DP-4162 - Honda	ISO-692 - ToolBOSCore message broker	Queue handler	Open	Injection of overflow	N/A	



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

