

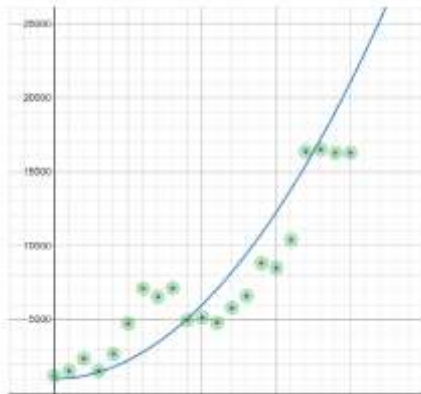
SOFTWARE-SCHWACHSTELLEN: ZUKÜNFTIGE HERAUSFORDERUNGEN

Andreas Harner
Abteilungsleiter CERT@VDE

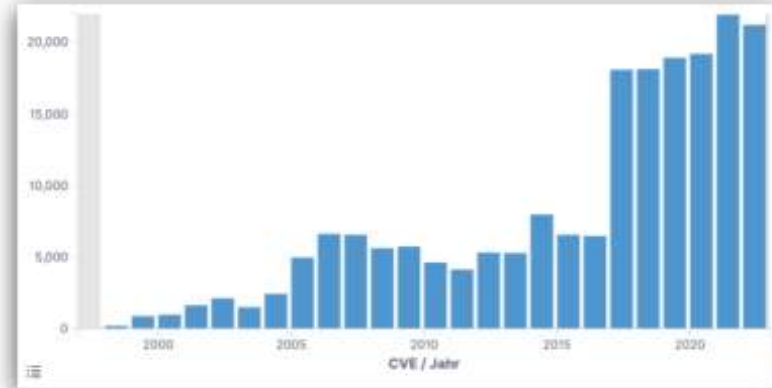


Web: <https://cert.vde.com>
Twitter: <https://twitter.com/certvde?lang=de>

„....Die Anzahl von Schwachstellen steigt...“

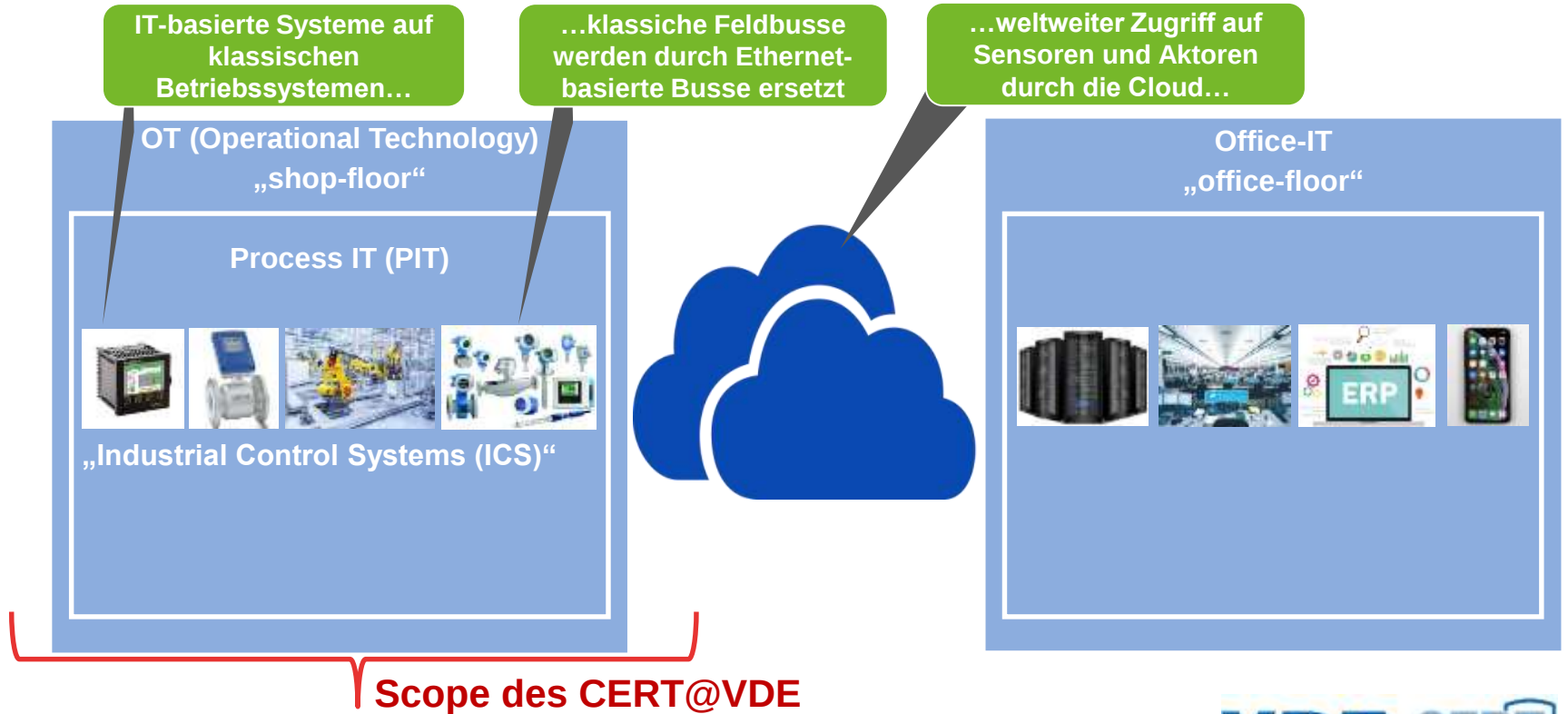


Quelle: <https://nvd.nist.gov>



<https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/>

Industrie 4.0, Smart xxx.....



Anforderung: Umgang mit Schwachstellen

- **IT-Grundschutz:** *IND.1.A12 Etablieren eines Schwachstellen-Managements*
[...] Grundlage dafür SOLLTEN Schwachstellenmeldungen (Advisories) von Herstellern [...] sein. [...]
- **ISO 27002:** Informationen über technische Schwachstellen von verwendeten Informationssystemen sollten rechtzeitig eingeholt, [...] bewertet und angemessene Maßnahmen [...] ergriffen werden.
- **IEC 62443-4-1:** DM-1: Empfang von Meldungen über sicherheitsbezogene Probleme
- **IEC 81001-5-1** Secure Health SW Lifecycle Process
- **IEC 60601-4-5:** Medical electrical equipment –Part 4-5: Guidance and interpretation – Safety-related technical security specifications (referenziert auf IEC 62443)

IEC 62443: Anforderungen zum Umgang mit Schwachstellen

General	Policies & Procedures	System	Component
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure product development lifecycle requirements
1-2 Master glossary of terms and abbreviations	2-2 IACS security program ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

 Published

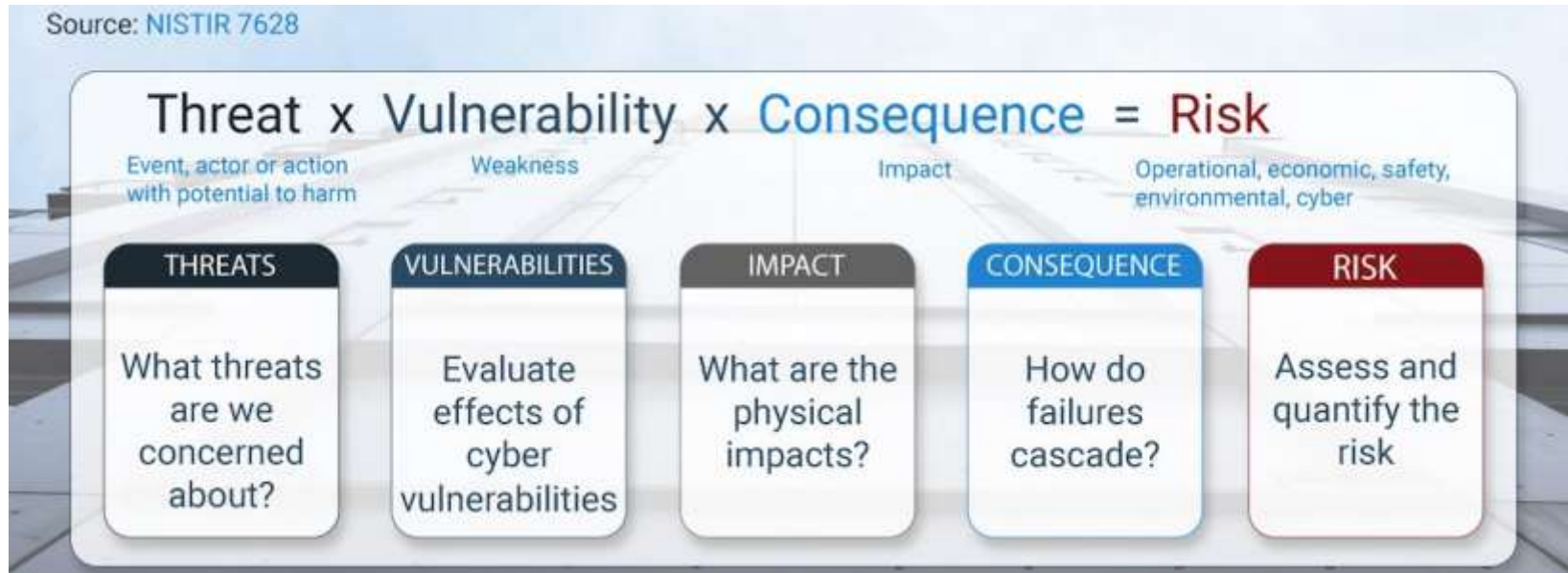
 Work in progress

Gesetzliche Anforderungen: Umgang mit Schwachstellen

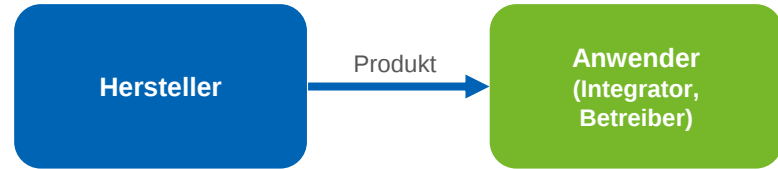
- **Heute:** bereits im deutschen Recht verankert
- **Zukünftig: EU-CRA**
 - CE-Kennzeichen für digitale Produkte,
 - Security-Anforderungen werden verpflichtend!
 - ohne dürfen die Produkte im EU-Binnenmarkt dann nicht mehr verkauft werden.
- **CRA: 3 Handlungsstränge:**
 - SBOMs
 - **Schwachstellen & CERTs**
 - Zertifizierung



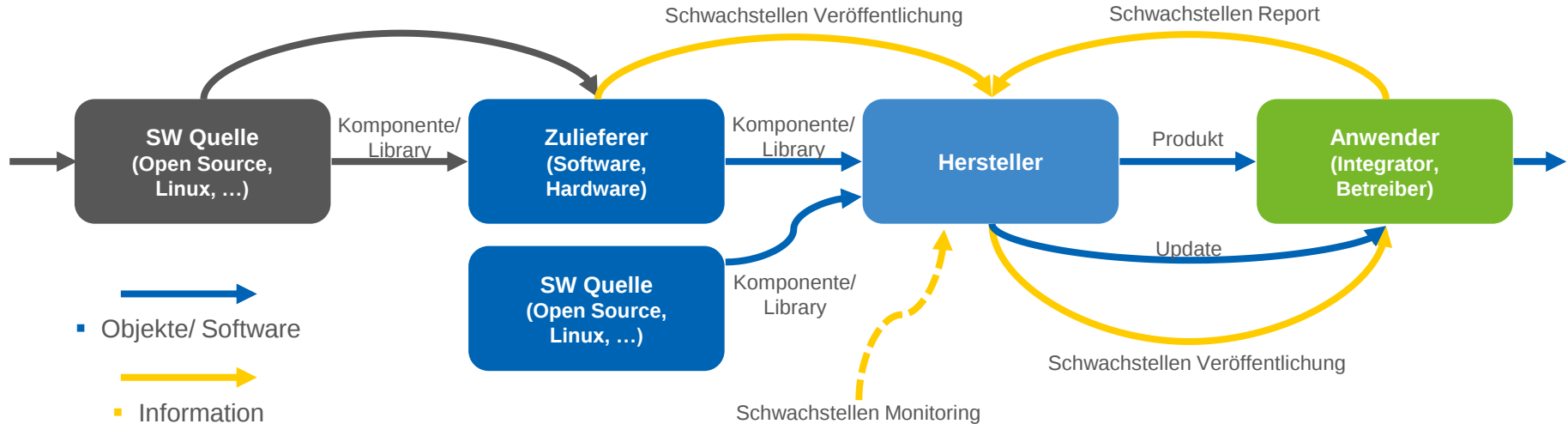
Schwachstellen veröffentlichen: ...damit mein Kunde sein Risiko kennt!



Beziehung Hersteller - Kunde → traditionell: „Einbahnstraße“



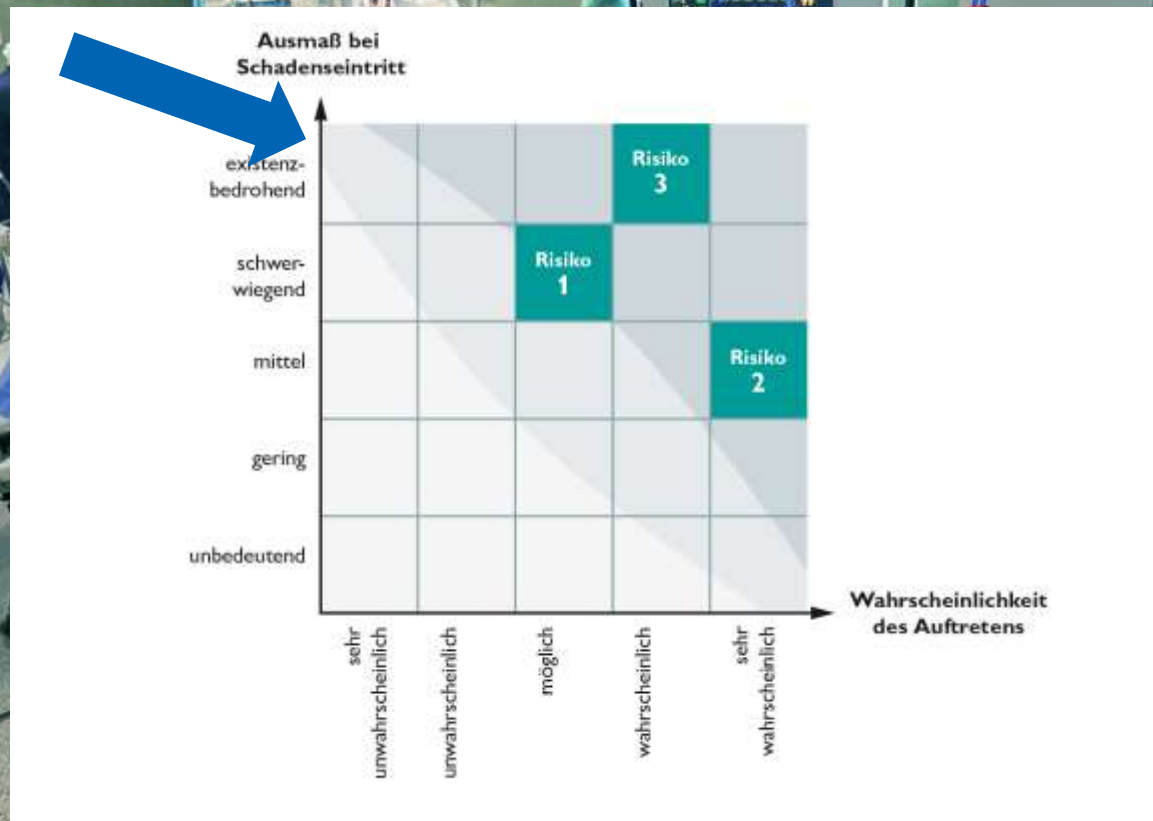
Beziehung Hersteller - Kunde → heute: Netzwerk



Angriffsziel OT: Herausforderung Risikobewertung



Angriffsziel „Krankenhaus-OT“: Herausforderung Risikobewertung



A photograph of an operating room. In the background, two surgeons in green scrubs and masks are performing an operation. The room is filled with medical equipment, including multiple monitors displaying vital signs and waveforms, IV stands with bags, and various cables. The lighting is bright, typical of a surgical suite.

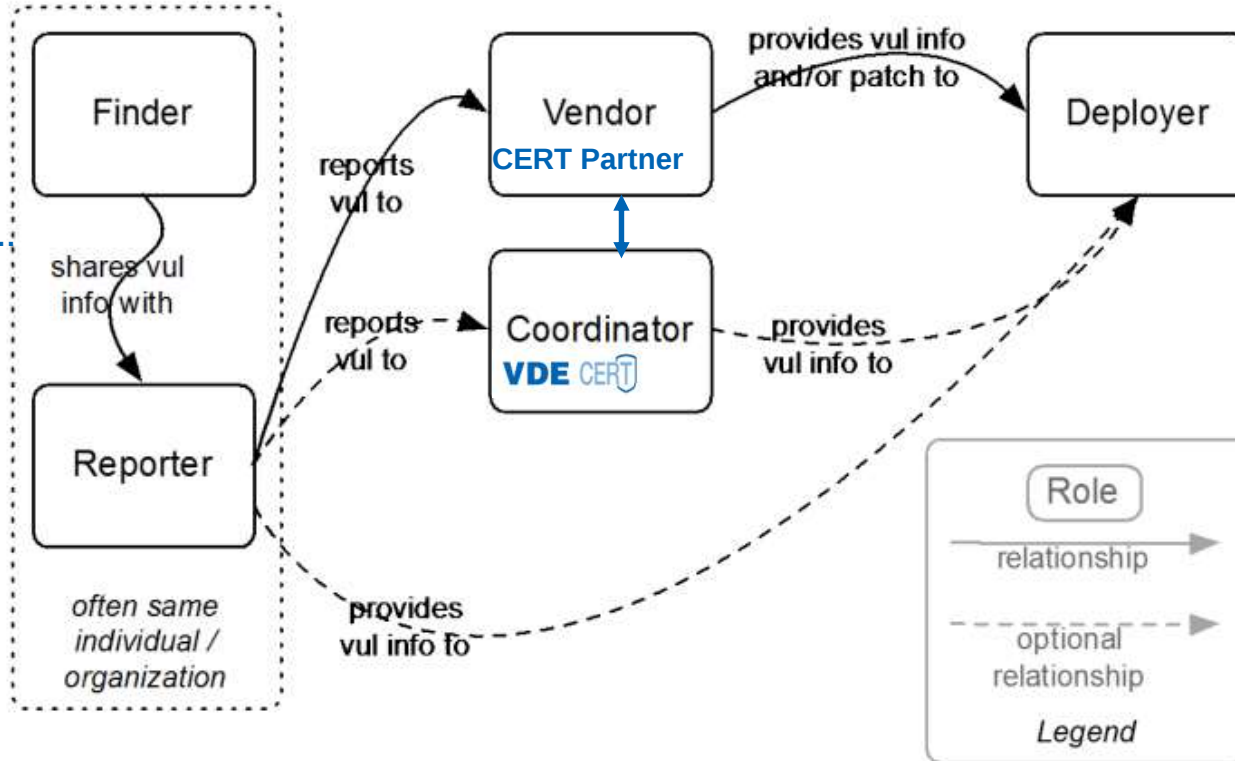
jeder Lieferant,
jede Automatisierungskomponente
jeder Mensch
...stellt ein mögliches Risiko dar.

Die Verantwortung geht damit auch auf
jeden Lieferanten über!!!

Coordinated Vulnerability Disclosure Prozess(CVD):

(Quelle: CMU)

Kunde,
Hacker,
Betreiber,
Forscher,
Hochschule
Konkurrenten...



Kunde, Betreiber, Anwender...

Coordinated Vulnerability Disclosure (CVD):

„Der CVD Prozess startet damit, dass mindestens eine Person Kenntnis von einer Schwachstelle in einem Produkt erlangt!“

→ Sofortige Zweiteilung der Welt:

Gruppe 1: ...die, die von der Schwachstelle wissen

Gruppe 2: ...die, die nix davon wissen

→ Gruppe 1 muss sich mit folgenden 2 Fragen beschäftigen:

Was muss als Antwort auf die Schwachstelle getan werden?

„NICHTS“

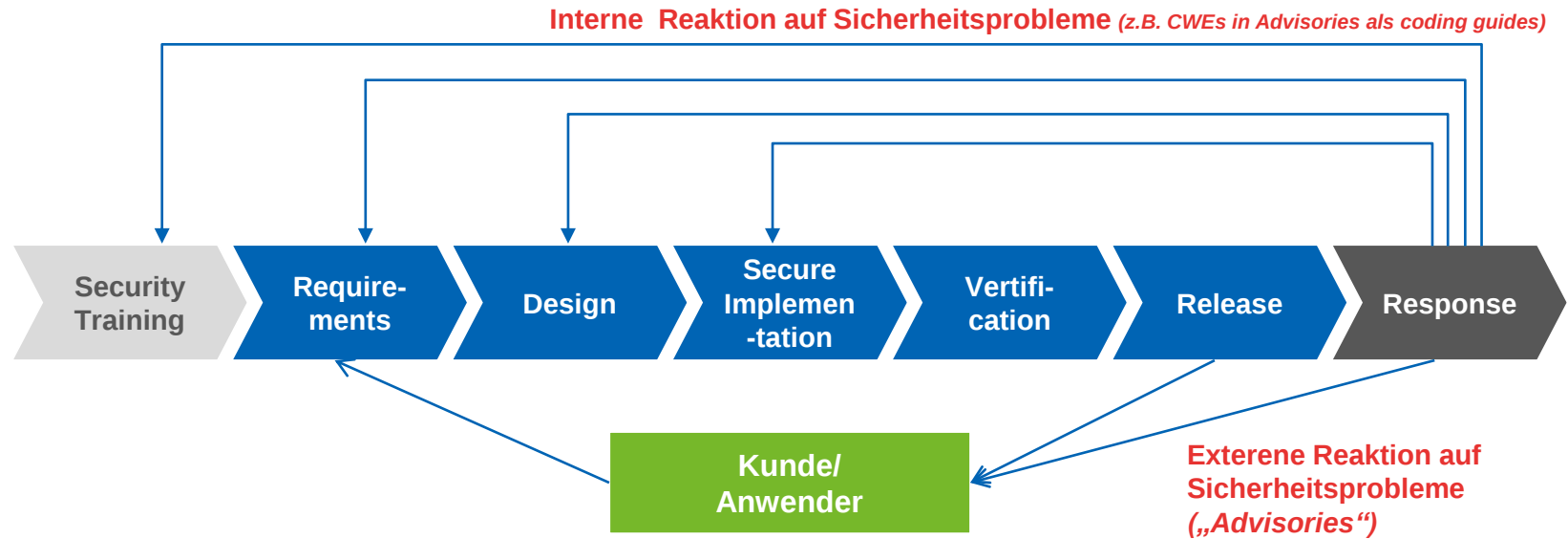
Wen muss man zusätzlich mit welcher Information versorgen?

„NIEMANDEN“

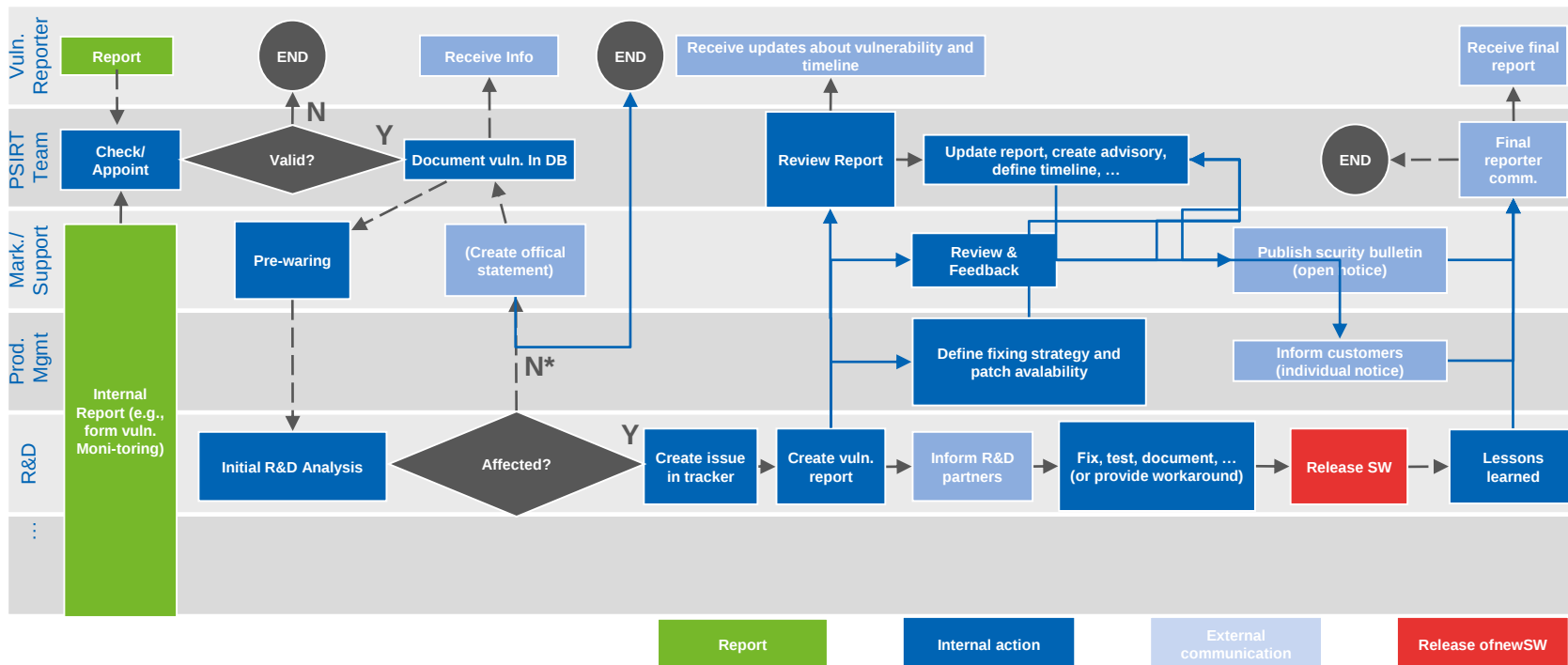
→ CVD Prozess läuft, solange die beiden Antworten „NICHTS“ und „NIEMANDEN“ lautet!

Interne und externe Reaktionen

- Was muss der Gerätehersteller intern tun, um sichere Software zu erzeugen?
- Wie muss der Gerätehersteller mit seinen Kunden und Zulieferern interagieren?



CERT@VDE – Response Process im kritischen Zeitfenster



Advisories

Sicherheitslücken treten immer wieder auf. Nur rechtzeitige Information ermöglicht es Nutzern und Administratoren, notwendige Maßnahmen zu ergreifen, um die Ausnutzung solcher Schwachstellen zu verhindern, da der Aufwand zur Behebung eines Schadens in den meisten Fällen wesentlich größer als der Aufwand zu dessen Vorbeugung ist. Diese Informationen werden in Form sog. Advisories veröffentlicht.

2. Mai 2022 12:00	zeige alle
TRUMPF: TruTops Fab, TruTops Boost prone to vulnerability	VDE-2022-018
27. April 2022 14:00	VDE-2022-015
Miele: Security vulnerability in Benchmark Programming Tool	
26. April 2022 14:00	VDE-2022-012
Pepperl+Fuchs: Vulnerability in multiple VisuNet devices	

Nachrichten

Hier informieren wir Sie über interessante und aktuelle Entwicklungen des CERT und halten Sie regelmäßig über Entwicklungen im Bereich IT-Sicherheit auf dem Laufenden.

5. April 2022 09:45	zeige alle
Security unter Kontrolle	
21. Januar 2022 12:45	
Website Update	
17. Januar 2022 11:21	
29. OFN-Konferenz „Sicherheit in vernetzten Systemen“	
15. Januar 2022 14:00	
Log4Shell / Log4J overview	

Dienstleistungen

Öffentliche Dienstleistungen

Schwachstelle melden

- via email (PGP-Public key)
- via Kontaktformular

Request a CVE-ID

- via email (PGP-Public key)
- via Kontaktformular

Partner



In Kooperation mit



Hersteller: wago / [Filter entfernen](#)

Vendor Feeds: [RSS / Atom](#)

2022-01-31 14:00

VDE-2022-002

WAGO: Vulnerable WIBU-SYSTEMS Codemeter installed through elCOCKPIT and WAGO-I/O-Pro

A vulnerability is reported in WIBU-SYSTEMS Codemeter. WIBU-SYSTEMS Codemeter is installed by default during elCOCKPIT and WAGO-I/O-Pro (CODESYS 2.3) installations. All currently existing elCOCKPIT installation bundles and WAGO-I/O-Pro (CODESYS 2.3) installation bundles are affected with vulnerable versions of WIBU-SYSTEMS Codemeter.

[weiter ...](#)

CVE-2021-41857, 7.1

2022-01-05 08:00

VDE-2021-060

WAGO: Smart Script affected by Log4Shell Vulnerability (Update A)

Apache Log4j is used for logging events in WAGO Smart Script in Version 4.2 and higher. Events logged by Log4j can contain

Feeds

[RSS / Atom](#)

Nach Hersteller

Beckhoff (8)

Bender (1)

Endress+Hauser (8)

Festo SE (1)

Helmholz (2)

Innominate (2)

Lenze (1)

MB connect line (7)

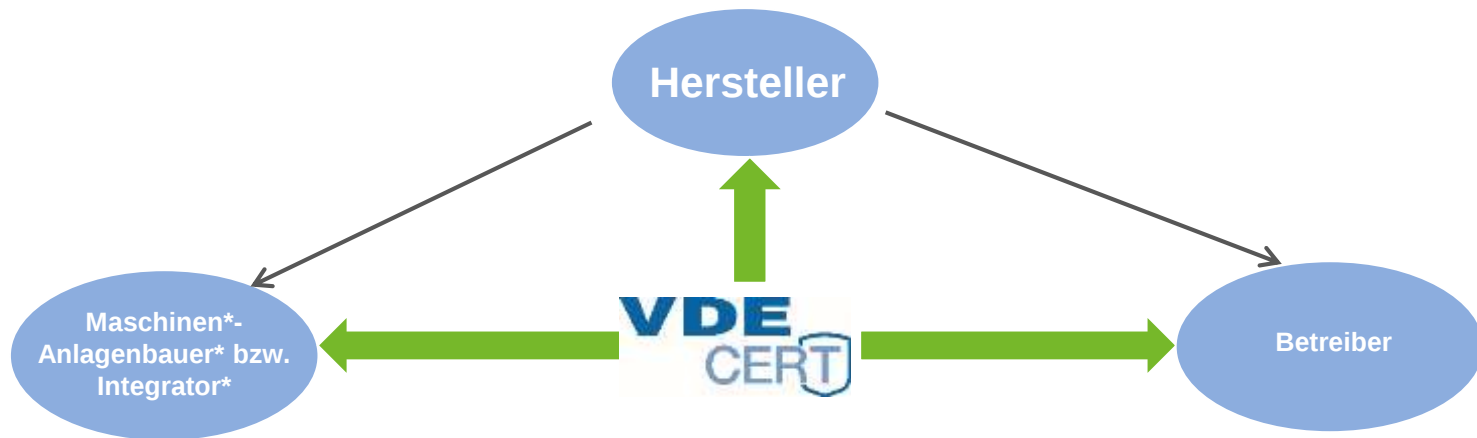
Miele (2)

M&M Software (1)

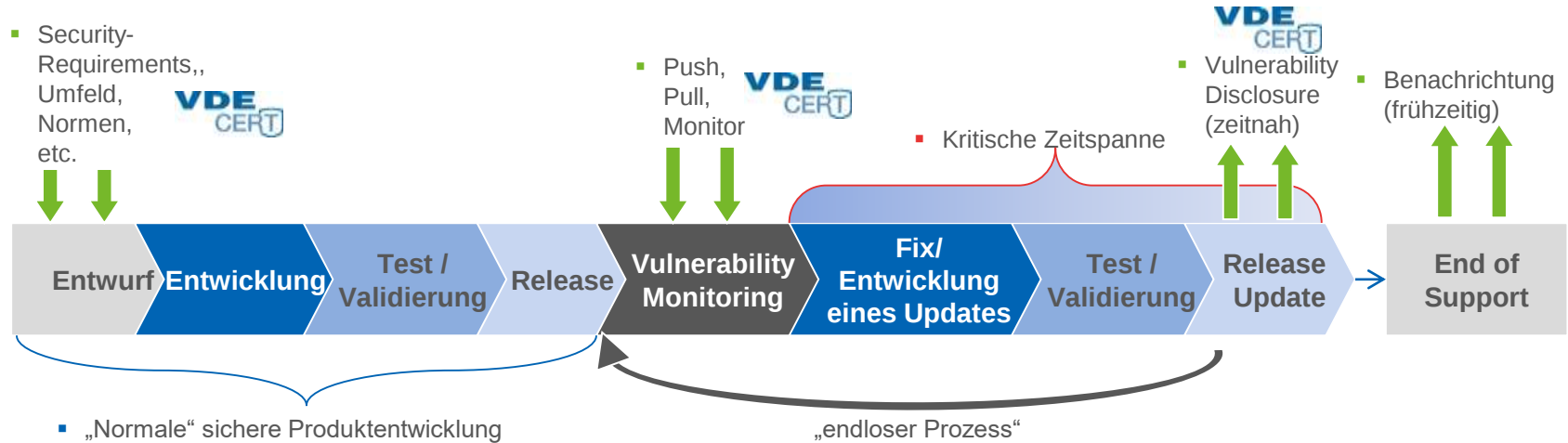
Pepperl+Fuchs (23)

PHOENIX CONTACT (50)

CERT@VDE: koordinierendes Produkt-CERT (PSIRT)



Produktlebenszyklus...und wo das CERT@VDE hilft



A world map illustrating the global distribution of COVID-19 cases. The size of the red circles represents the number of cases in each country. The United States has the largest circle, followed by Spain and Italy. Other countries with significant case counts include France, Germany, and the United Kingdom. The map also shows smaller circles for countries like Canada, Mexico, Brazil, and various nations in Europe, Africa, and Asia. The oceans are labeled in blue text: ATLANTIC OCEAN, PACIFIC OCEAN, INDIAN OCEAN, and ARCTIC OCEAN. Country names are labeled in black text.

CERT@VDE ist anerkannte “CVE Numbering Authority (CNA)“:

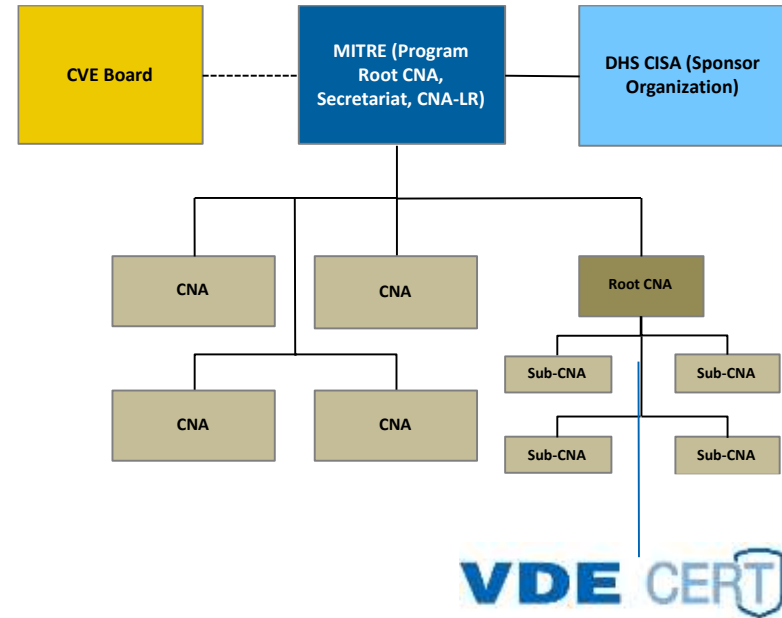
Vergabe von CVE Nummern!

Vorteile

- Kontrolle des kompletten CVE-Veröffentlichungsprozess aus dem Scope des CERT@VDE
- ***Kein Teilen von Embargoinformationen mit anderer CNA notwendig!***
- Beschleunigter Vulnerability Disclosure Prozess

Voraussetzung:

- Öffentlich zugängliche Disclosure Policy
- Positives Durchlaufen des CNA Anerkennungsprozesses bei MITRE
- Anerkennung und Beherrschen der CNA Regularien und Prozesse



Status quo: wie CERTs heute arbeiten...

The screenshot shows the CISA website with the header "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY". The main content area displays the "ICS Advisory (ICSA-21-138-01)" for "Emerson Rosemount X-STREAM". The advisory is dated May 18, 2021. Below the advisory title, there are social media links for LinkedIn, Facebook, and Twitter. The advisory is categorized under "Legal Notice". The main body of the advisory is titled "1. EXECUTIVE SUMMARY" and contains the following information:

- CVE ID:** CVE-2021-22741
- Severity:** Critical
- Vendor:** Emerson
- Equipment:** Rosemount X-STREAM Gas Analyzer
- Vulnerability:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Incomplete Restriction of Retrieved UI Layers or Frames

The advisory also includes a "2. RISK EVALUATION" section and a "3. TECHNICAL DETAILS" section, with the first subsection being "3.1 AFFECTED PRODUCTS".



Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

11 May 2021

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The **EcoStruxure Geo SCADA Expert** product is an open, flexible and scalable software system for telemetry and remote SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

Affected Products and Versions

- ClearSCADA, all versions
- EcoStruxure Geo SCADA, all versions
- EcoStruxure Geo SCADA, all versions

Vulnerability Details

CVE ID: CVE-2021-22741

CSS v3.1 Base Score: 5.7

A-CWE-815: Use of Passwords that could cause the system to be vulnerable to password attacks.

Exploitation of this vulnerability could result in unauthorized access to the system.

Remediation

Geo SCADA Expert 2020 April 2021 (83.787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:

<https://www.schneider-electric.com/energy/energy/en/Products/SCADA-Expert/Security>

Installation of new server software will require system restart or changes of redundant servers. Consult the Release Notes and Resource Center for advice on this procedure.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or in an offline infrastructure.

11 May 21

Document Reference Number - SEVD-2021-138-01

Page 1 of 1

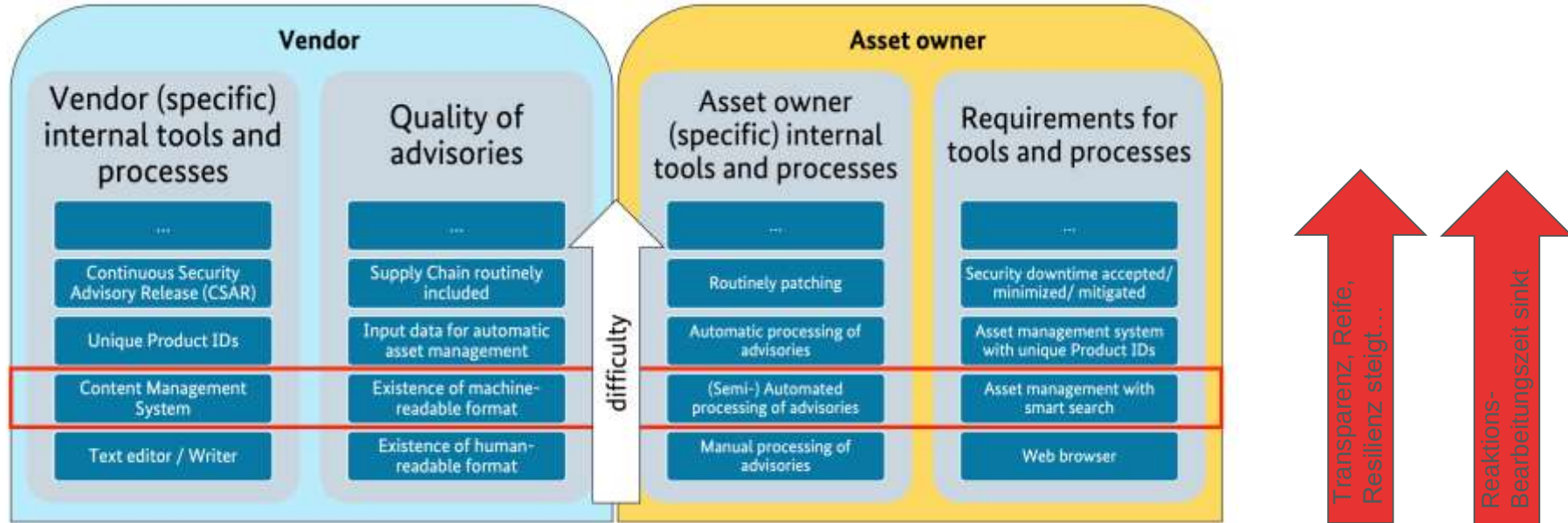


The screenshot shows a Schneider Electric security notification for the EcoStruxure Geo SCADA Expert product. The notification is dated May 11, 2021, and is titled "Schneider Electric Security Notification". The main content area displays the "EcoStruxure Geo SCADA Expert" product. The notification is categorized under "Overview". The main body of the notification is titled "1. EXECUTIVE SUMMARY" and contains the following information:

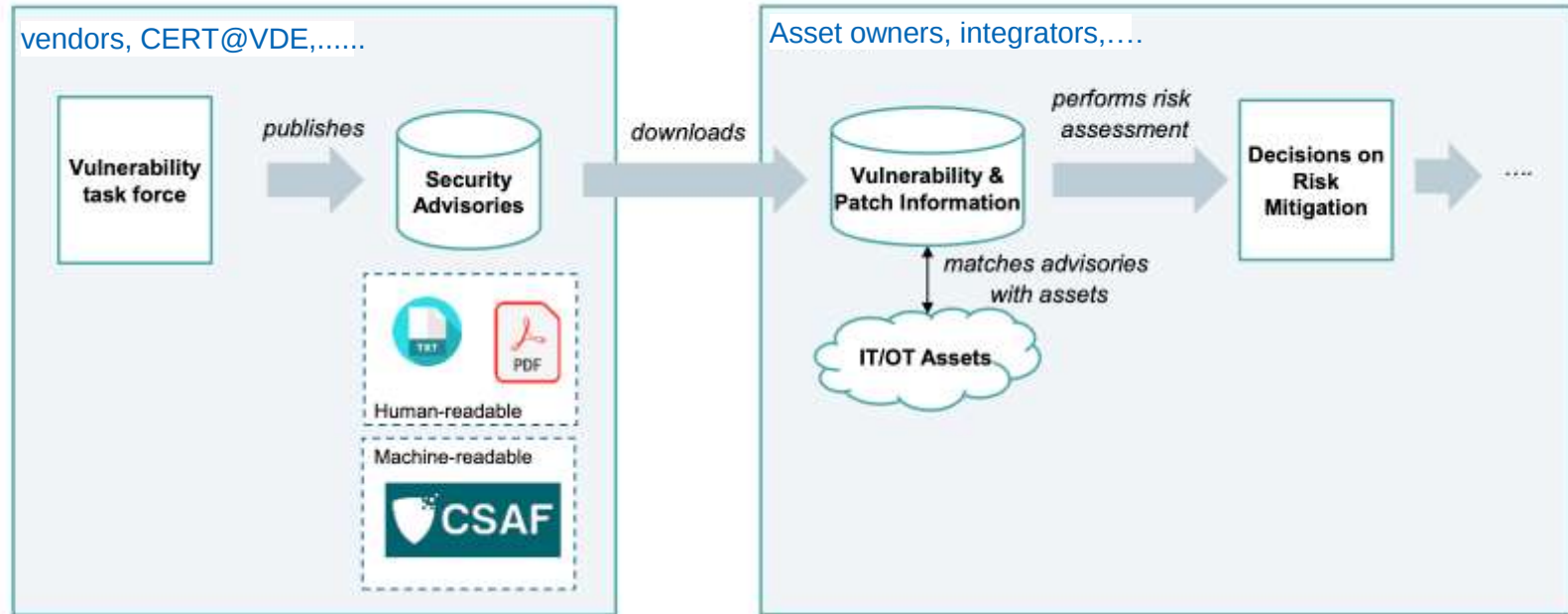
- CVE ID:** CVE-2021-22741
- Severity:** Critical
- Vendor:** Schneider Electric
- Equipment:** EcoStruxure Geo SCADA Expert
- Vulnerability:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Incomplete Restriction of Retrieved UI Layers or Frames

The notification also includes a "2. RISK EVALUATION" section and a "3. TECHNICAL DETAILS" section, with the first subsection being "3.1 AFFECTED PRODUCTS".

Nächster Schritt mit CSAF

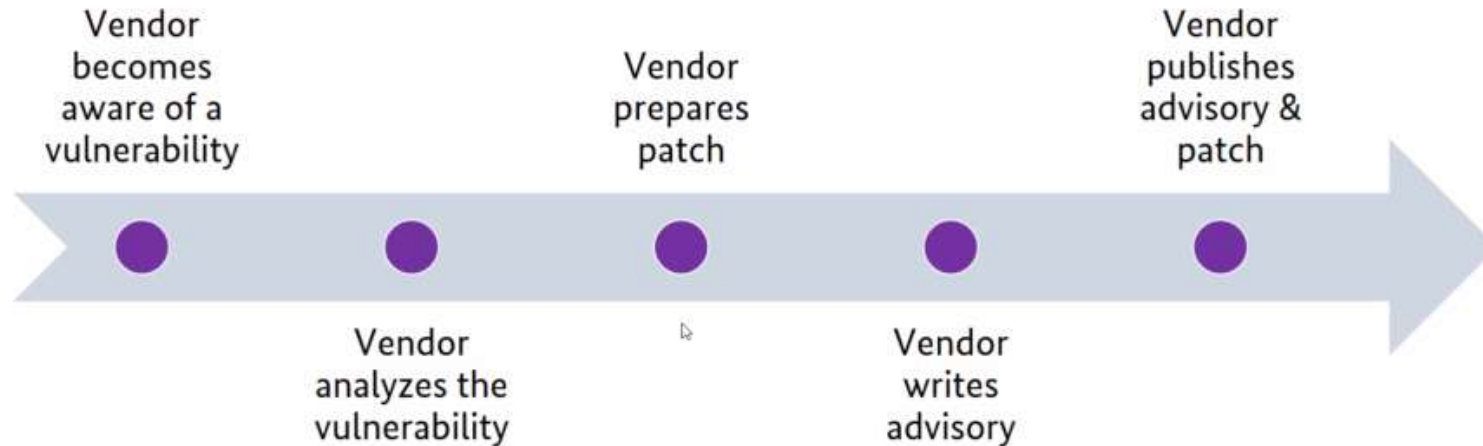


CSAF (Common Security Advisory Framework): → maschinenlesbares Advisory Format!



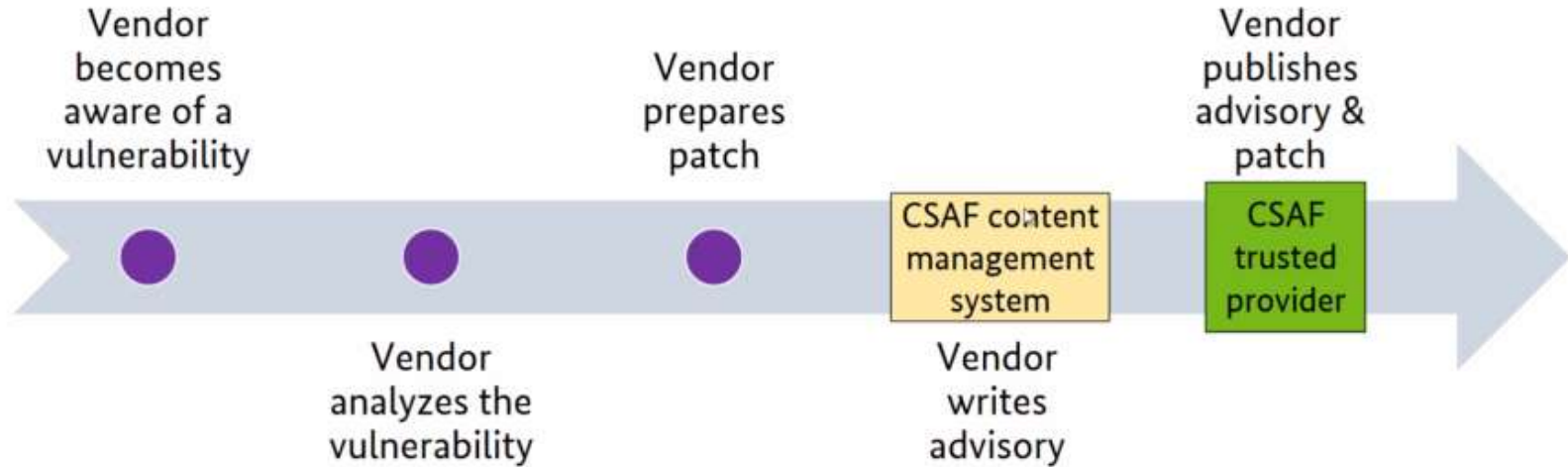
Hersteller - heute

Source: Thomas Schmidt (BSI)



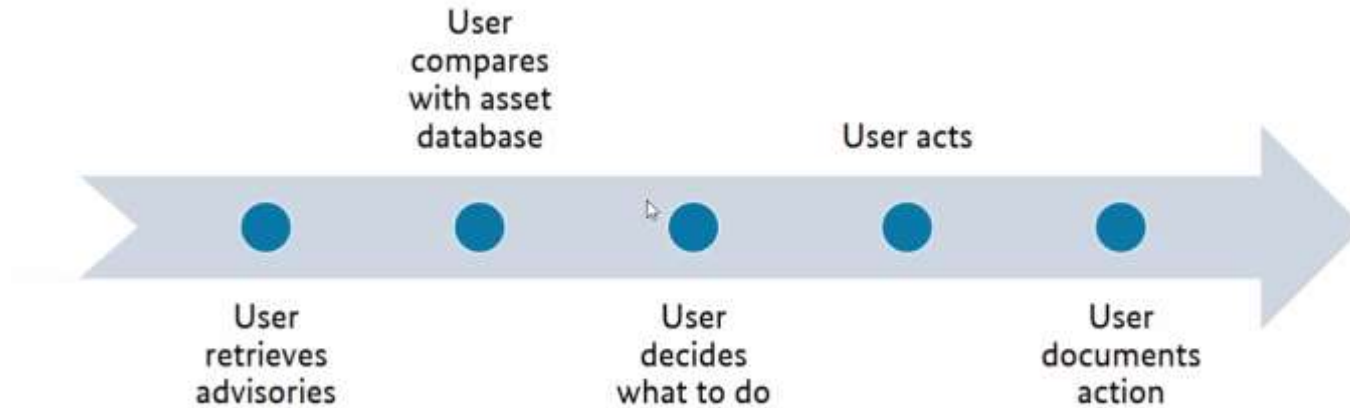
Hersteller - zukünftig

Source: Thomas Schmidt (BSI)



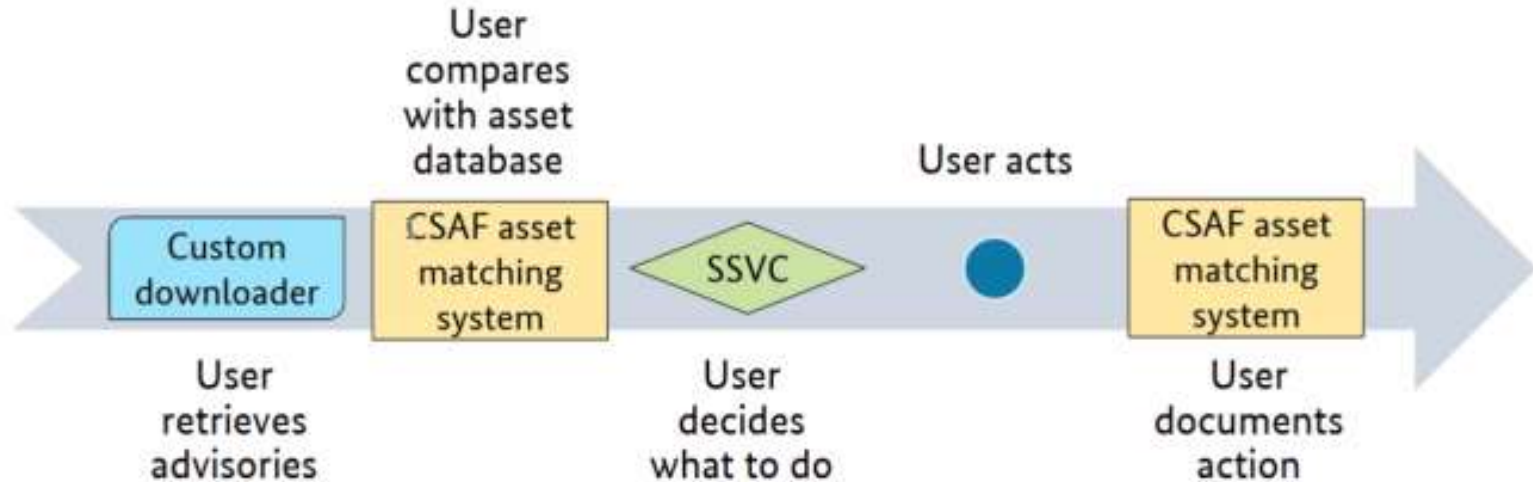
Betreiber - heute

Source: Thomas Schmidt (BSI)



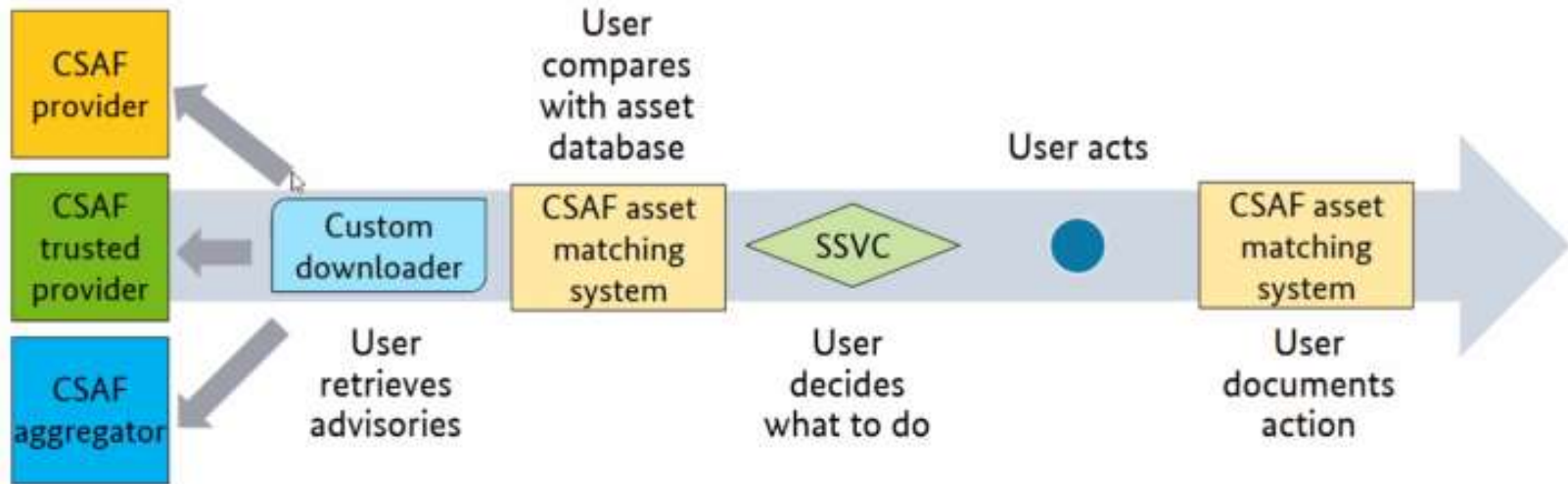
Betreiber - zukünftig

Source: Thomas Schmidt (BSI)

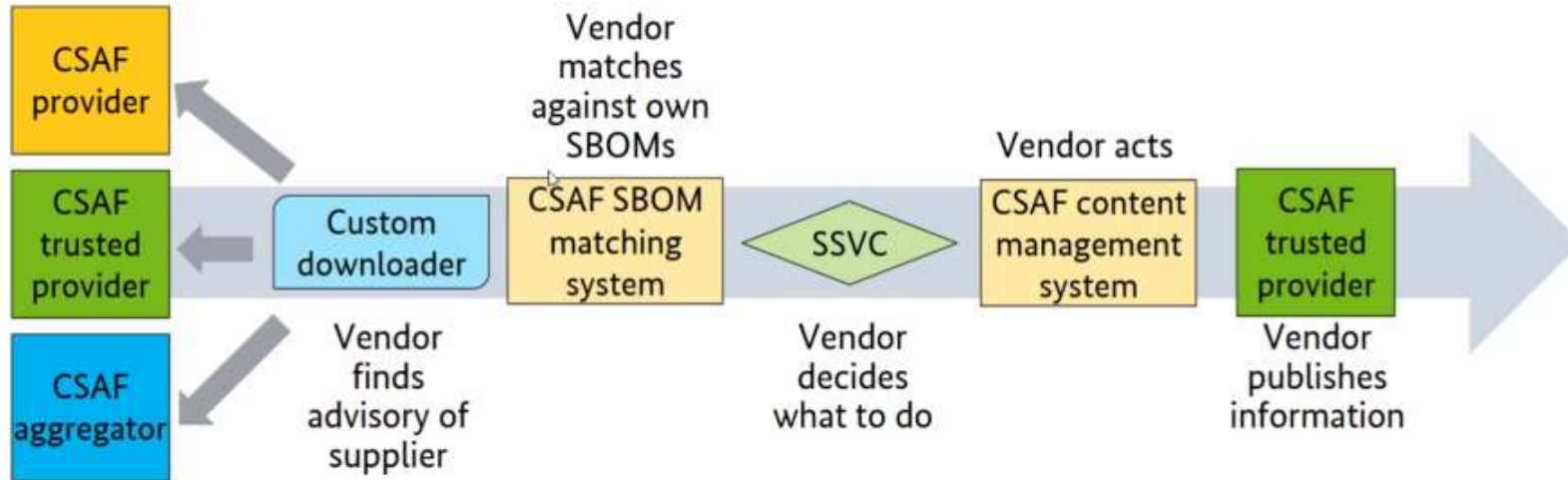


Betreiber - zukünftig

Source: Thomas Schmidt (BSI)

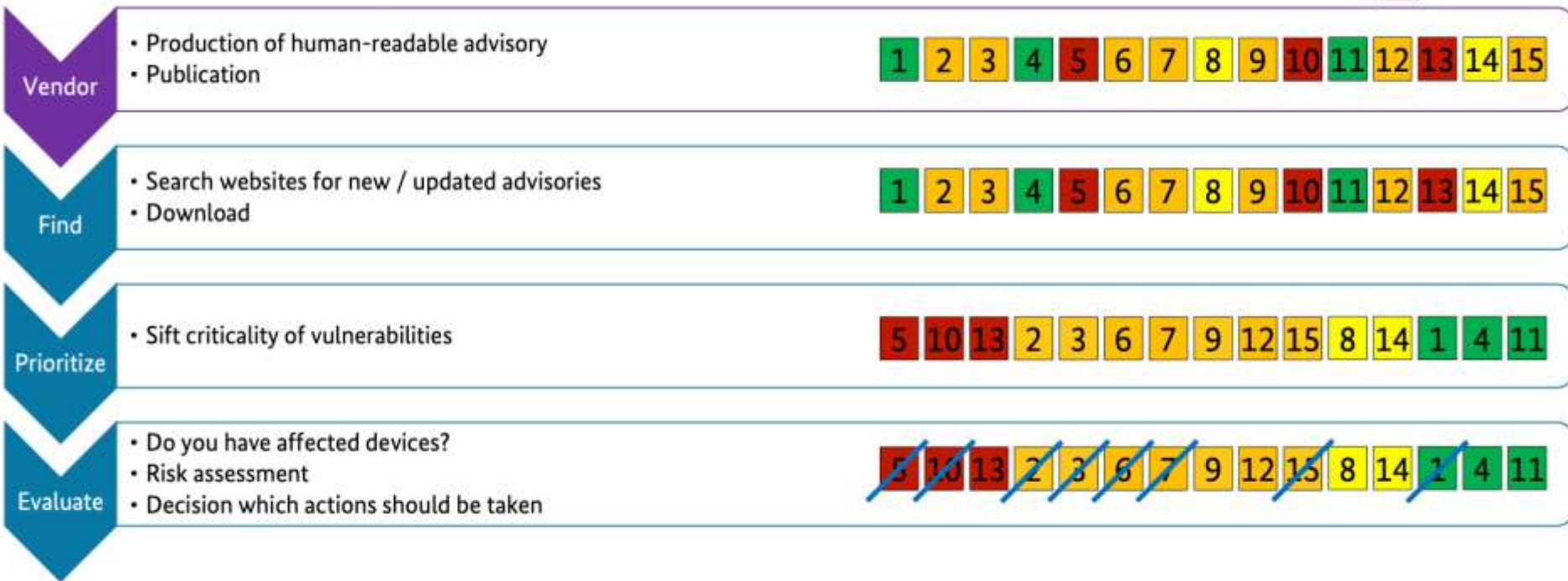


Hersteller ist auch Integrator und Betreiber!



Schwachstellen-Handling: manuelle Prozesse bei Anwendern!

Source: Thomas Schmidt (BSI)



Severity of advisory

- low
- medium
- high
- critical

Schwachstellen-Handling mit CSAF...

Source: Thomas Schmidt (BSI)

Vendor

- Production of machine-readable advisory
- Publication

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Find

- Search websites for new / updated advisories
- Download

automated

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Evaluate
(static)

- Do you have affected devices?
- Risk assessment (static) => adopt criticality
- Criticality of the vulnerability

automated

~~5~~ ~~10~~ ~~13~~ ~~2~~ ~~3~~ ~~6~~ ~~7~~ 9 12 ~~15~~ 8 14 ~~1~~ 4 11
13 9 14 4 8 12 11

Measures

- Sift of advisories with affected devices sort by criticality
- Decision which actions should be taken

13 9 14 4 8 12 11

Severity of advisory
low
medium
high
critical

Resümee

- Sicherheit wird „nicht weggehen“
- Sicherheit ist nicht nur **Produkt/Technik, sondern viel Prozess**
- Es ist Arbeit und berührt alle Bereiche eines Unternehmens
- ... aber: Jeder kann es umsetzen..
 - Teile der Arbeiten können/müssen **automatisiert** werden
 - man muss **nicht alles selbst** tun: CERT@VDE

Resümee

.....

■ Risikominimierung durch ...

- *klare Kommunikation, nachvollziehbare Prozesse und operativer Austausch („Community der Handelnden“)*
- *CERT ist „Informationsmanagement“: zielgruppenorientiert!*
- *Frühwarnung*
- *Best Practices*
- *CVD: Offener Umgang mit Schwachstellen*
- *CERT ist „Krisenstab“ und nicht die „Eingreiftruppe“!*
- *CERT organisiert Hilfe-zur-Selbsthilfe → „organisationales Lernen“*

! Frühwarnsystem und Wissensvorsprung

Frühzeitigeres Erkennen von Schwachstellen ermöglicht Partnern eine bessere Einschätzung! ...und dadurch eine schnelle, strukturierte Reaktion auf aktuelle Bedrohungen!

⚖️ Minimierung Haftungsrisiken

- Best Practices des CERT@VDE unterstützen die Einhaltung von rechtlichen Vorgaben hinsichtlich „im Verkehr erforderliche Sorgfalt“ und „Stand der Technik“
- Vertragliche und gesetzliche Produktbeobachtungspflichten der Partner werden unterstützt
- Das CERT@VDE hilft auch bei Kritis-Fällen, um die richtigen Wege zu gehen

🔧 Positives Firmenimage bei den Kunden

Teilnehmende Partner dokumentieren verantwortungsbewussten Umgang mit IT-Sicherheit

🧠 Prozesse – Erfüllung von normativen Anforderungen

- CERT@VDE stellt Partnern abgestimmte und solide Prozesse zur Verfügung
- Partner können diese Prozesse in eigene, übergeordnete Security-Prozesse integrieren
- Dadurch u.a. Hilfe bei der Umsetzung der IEC 62443



Zentrale Kontaktstelle...

- ..für Hersteller, Maschinenbauer (Integratoren), Betreiber
- ..für Behörden (z. B. BSI, Verfassungsschutz)
- ..für andere CERTs, CERT-Verbund
- ..für Security Consultants, Hacker und Sicherheitsforscher



Advisory-Service – und CNA

Unterstützung der Partner durch routinierte Security-Experten:

- CVD Prozess: koordinierte, abgestimmte Veröffentlichung
- Interaktion in deutscher und englischer Sprache
- Koordination mit anderen CERTs (z. B. ICS-CERT)
- CERT@VDE ist eine von Mitre anerkannte CNA (CVE Numbering authority) und übernimmt für seine Partner die entsprechenden Aufgaben
- Zukünftig CSAF Publisher/Provider/Aggregator



Security Development Lifecycle

Partner können Schwachstelleninformationen über CWEs in Planung, Entwicklung und Modellierung neuer Produkte berücksichtigen ("Security-by-Design")



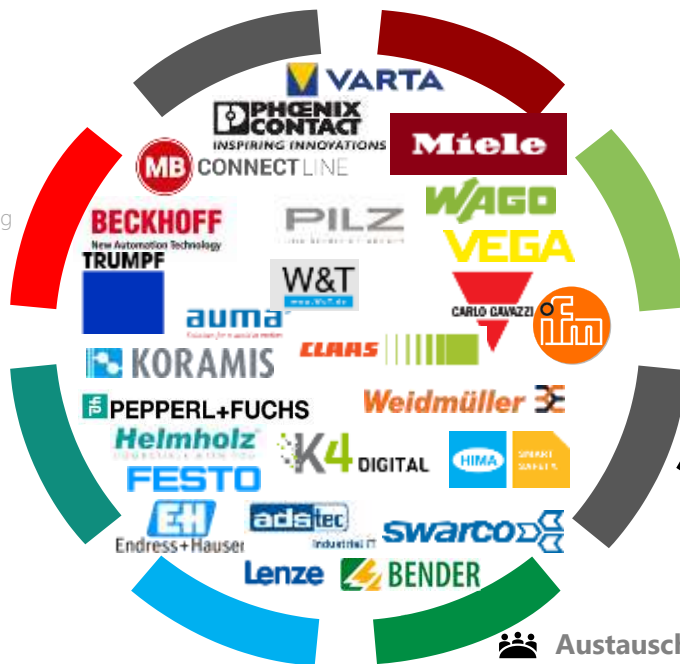
Partnerschaften und Akkreditierung

- CERT@VDE ist akkreditiert durch den europäischen Trusted Introducer
- CERT@VDE ist Mitglied im Deutschen CERT Verbund



Austausch - Vernetzung – Hilfe:

- herstellerübergreifend, vertrauenswürdig und sicher
- anonymisiert (auf Wunsch) und in gleicher Zeitzone
- gemeinsame Workshops und Best Practices und operative Arbeit in TLP:RED Fokusgruppen
- Informationsmanagement und Interessensvertretung für die Partner in Richtung der (inter)nationalen CERT-Community



Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Andreas Harner

Leiter CERT@VDE

Tel. +49 69 6308-392

andreas.harner@cert.vde.com

