SIEMENS

Einhaltung des Cyber Resilience Act

Unterstützung und Lösungen, um gemeinsam die Cybersecurity-Vorschriften zu bewältigen!

Cyber Resilience Act (CRA) – Verpflichtungen*

Sicherheitsfunktionen
Standardmäßig sicher | Schutz vor unbefugtem Zugriff | Gewährleistung von Datenintegrität und -vertraulichkeit | Widerstandsfähigkeit gegen DoS-Angriffe | Begrenzung der Angriffsfläche | Mechanismen für sichere Updates ...

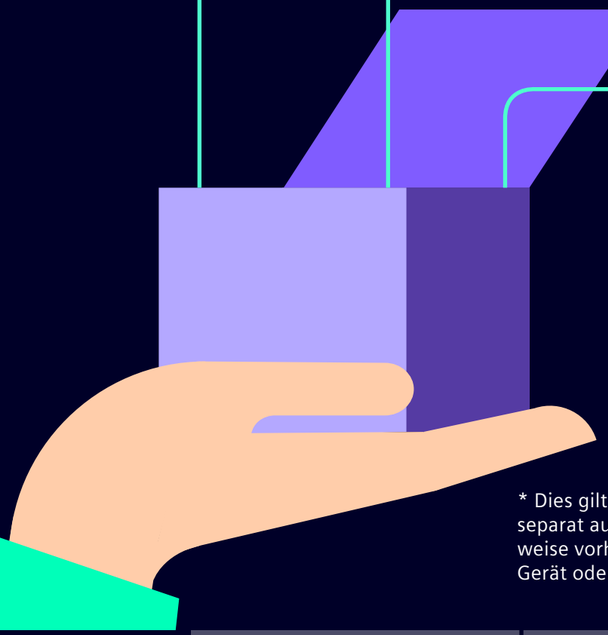
Dokumentation
Interne technische Dokumentation (Konformität, Testergebnisse usw.) | Informationen und Anweisungen für Benutzer (Verwendungszweck, Umgebung, sichere Konfiguration)

Lebenszyklusprozess
Bewertung von Cybersecurity-Risiken | Bereitstellung von Updates | Festgelegte Support-Zeiträume ...

Meldung
... von aktiv ausgenutzten Schwachstellen | ... von schwerwiegenden Vorfällen, die Auswirkungen auf die Sicherheit des Produkts haben

Umgang mit Sicherheitslücken
Regelmäßige Tests | Öffentliche Bekanntgabe von Informationen zu Sicherheitslücken | Angabe einer Kontaktadresse ...

Konformitätsbewertung
Je nach Produktklassifizierung: Alleinige Selbstdeklaration oder Einbeziehung einer benannten Stelle



* Dies gilt für jedes Software- oder Hardwareprodukt und dessen Lösungen zur Fernverarbeitung von Daten, einschließlich separat auf den Markt gebrachten Software- oder Hardwarekomponenten, deren bestimmungsgemäßer oder vernünftigerweise vorhersehbarer Verwendungszweck eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netzwerk umfasst.

Quelle:
Verordnung 2024/2847 – DE – EUR-Lex. Siehe Anhang I „Wesentliche Cybersicherheitsanforderungen“

Meldepflichten

Art der Meldung	Aktiv ausgenutzte Schwachstellen	Schwere Vorfälle
Frühwarnung	< 24 h	< 24 h
Sicherheitslücke/ Vorfallmeldung	< 72 h	< 72 h
Abschlussbericht	< 14 Tage nach Verfügbarkeit einer Korrektur-/Abhilfemaßnahme	< 14 Tage nach Einreichung der Vorfallsmeldung

Quelle:
Verordnung 2024/2847 – DE – EUR-Lex
(siehe Meldepflichten der Hersteller, Artikel 14)

Übersicht über spezifische CRA-Anforderungen und -Verpflichtungen

Die CRA legt wesentliche Verpflichtungen für Hersteller fest, sichere Produkte auf den Markt zu bringen und deren Sicherheit während des gesamten Lebenszyklus zu gewährleisten. Diese Verpflichtungen lassen sich in drei Hauptkategorien einteilen: sichere Lebenszyklusprozesse, Schwachstellenmanagement und Sicherheitsfunktionen. Jede Kategorie hat spezifische technische und verfahrenstechnische Anforderungen.

Lebenszyklusprozess

Der Cyber Resilience Act verpflichtet Hersteller dazu, während des gesamten Produktlebenszyklus sichere Entwicklungsprozesse zu implementieren. Zu diesen Prozessen gehören die Durchführung von Cybersicherheits-Risikobewertungen, die Pflege von Dokumentationen und Berichten, die Festlegung von Support-Zeiträumen sowie die Durchführung von Konformitätsbewertungen. Diese Maßnahmen gewährleisten, dass Sicherheit vom Entwurf bis zum Ende der Lebensdauer integriert ist und die Konformität durch detaillierte technische Dokumentationen nachgewiesen werden kann.

Sicherheitsfunktionen

Um die CRA-Anforderungen zu erfüllen, müssen Produkte über wesentliche Cybersecurity-Funktionen verfügen. Dazu gehören sichere Authentifizierung, Datenintegrität und -vertraulichkeit, Minimierung der Angriffsfläche, Protokollierung von Sicherheitsereignissen sowie Widerstandsfähigkeit gegen Denial-of-Service-Angriffe. Darüber hinaus müssen Hersteller für sichere Standardkonfigurationen sorgen, Updates ermöglichen und das Risiko begrenzen, dass ein Produkt andere Produkte gefährdet. So wird eine starke Sicherheitsbasis im gesamten digitalen Ökosystem gewährleistet.

Umgang mit Sicherheitslücken

Laut CRA sind Hersteller dafür verantwortlich, Sicherheitslücken in ihren Produkten zu identifizieren und zu beheben. Dazu gehören regelmäßige Sicherheitstests, um sicherzustellen, dass Produkte ohne bekannte Sicherheitslücken ausgeliefert werden, sowie die Offenlegung relevanter Informationen zu Sicherheitslücken. Um die Produktintegrität langfristig zu gewährleisten, müssen Unternehmen außerdem eine Kontaktstelle bereitstellen, zeitnahe Updates anbieten und Mechanismen für die sichere Verteilung dieser Updates einrichten.

Lösungen auf Basis des Cybersecurity-Leitfadens für Maschinenhersteller

Lebenszyklusprozess

- CRA Consulting
- Lifecycle Management
- Risk Assessment

Sicherheitsfunktionen

- Perimeter Protection
- Authentication and Access Control
- Event Logging
- Integrity and Confidentiality
- Hardening

Umgang mit Sicherheitslücken

- Security Testing and Scanning
- Vulnerability Discovery and Management
- Vulnerability Management Services

CRA Consulting
Von der Einhaltung gesetzlicher Vorschriften bis hin zu DevSecOps

Beispiel

1 **Selbstbewertung**
Führen Sie eine Anwendbarkeitsbewertung durch, um zu klären, ob Ihre Produkte unter die CRA fallen

2 **Kategorisierung**
Wählen Sie die Kategorie des Produkts anhand seiner Funktionen aus und überprüfen Sie anschließend die Anwendbarkeit der CRA

3 **Konformität herstellen**
Risikobewertung durchführen und das Produkt mit den wesentlichen Cybersecurity-Anforderungen in Einklang bringen

4 **Erstellung der Dokumentation**
Erstellen Sie die erforderliche technische Dokumentation einschließlich Anweisungen für Benutzer

5 **Formelle Verfahren**
Durchführung der ausgewählten Konformitätsbewertungsverfahren, Erhalt der EU-Konformitätserklärung und der CE-Kennzeichnung

6 **Kontinuierliche Überwachung**
Befolgung von Melde-, Überwachungs- und Berichtspflichten

CRA-Konformität für Maschinen
Siemens unterstützt Sie mit einer maßgeschneiderten, risikobasierten Roadmap auf dem Weg zur CRA-Konformität.

Wir können Ihnen dabei helfen, die Einhaltung folgender Vorschriften sicherzustellen:

- Produktrisikobewertung und Produktkonformität ✓
- Aufrechterhaltung der Produktsicherheit über den gesamten Lebenszyklus hinweg ✓
- Einhaltung von Vorschriften und Erfüllung von Berichtspflichten ✓
- Einführung von DevSecOps ✓
- Einrichtung einer Organisation für Lösungssicherheit ✓

Cybersecurity Lifecycle Management

Durchgängige Rückverfolgbarkeit | Secure by Design | Bereit für CRA

Einheitliche Rückverfolgbarkeit über den gesamten Lebenszyklus

Polarion verknüpft Cybersecurity-Anforderungen, Entwicklungsartefakte, Schwachstellen und Maßnahmen über den gesamten Lebenszyklus. Es automatisiert Software BoM (SBOM) und Dokumentation, bietet vollständige Nachverfolgbarkeit und unterstützt die CRA-Konformität.

Risikomanagement

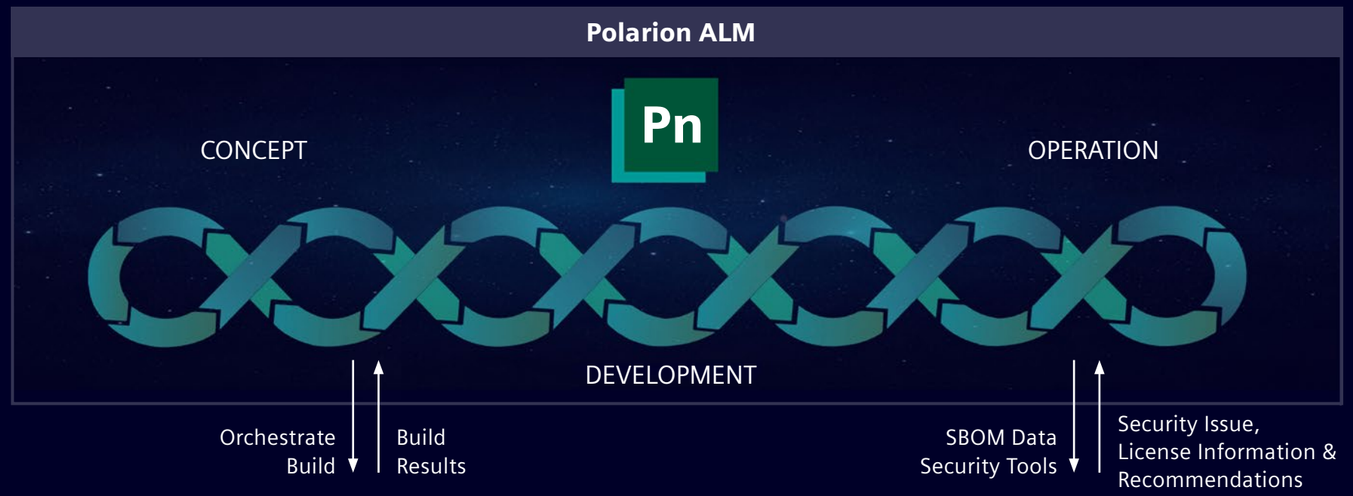
Identifiziert und priorisiert Cybersecurity-Risiken im Produktkontext und verknüpft Schwachstellen mit betroffenen Komponenten, Anforderungen und Maßnahmen – inklusive Risiken durch Dritte und in der Lieferkette.

Integrierte Analyse

Konsolidiert Eingaben aus Entwicklungs- und Sicherheitstools, um eine frühzeitige Wirkungsanalyse, fundierte Entscheidungen und Secure-by-Design-Praktiken während der gesamten Entwicklung zu ermöglichen.

Durchgängiges SBOM-Management

Automatisiert SBOM-Erfassung und -Synchronisierung und schafft kontinuierliche Transparenz zu Komponenten, Lizenzen und Schwachstellen. Unterstützt CRA-Vorgaben und Standards mit integrierten Tools wie Vilocify.



Build & Automation Tools & Code Repository (examples)

Jenkins · GitHub · SVN · SIEMENS SIMATIC · git · Bitbucket · Azure DevOps

Software Security Tools

Vilocify or 3rd Party Tools

Cybersecurity-Managementsystem Bibliotheken zu Bedrohungen und Schäden Bedrohungs- und Risikobewertung	Software-BOM-Management Vollständige Code-Analyse SBOM-Abgleich und -Scan	Rückverfolgbarkeit „Verwendung“ Kontinuierliche Qualitätssicherung Analyse der Auswirkungen von Schwachstellen

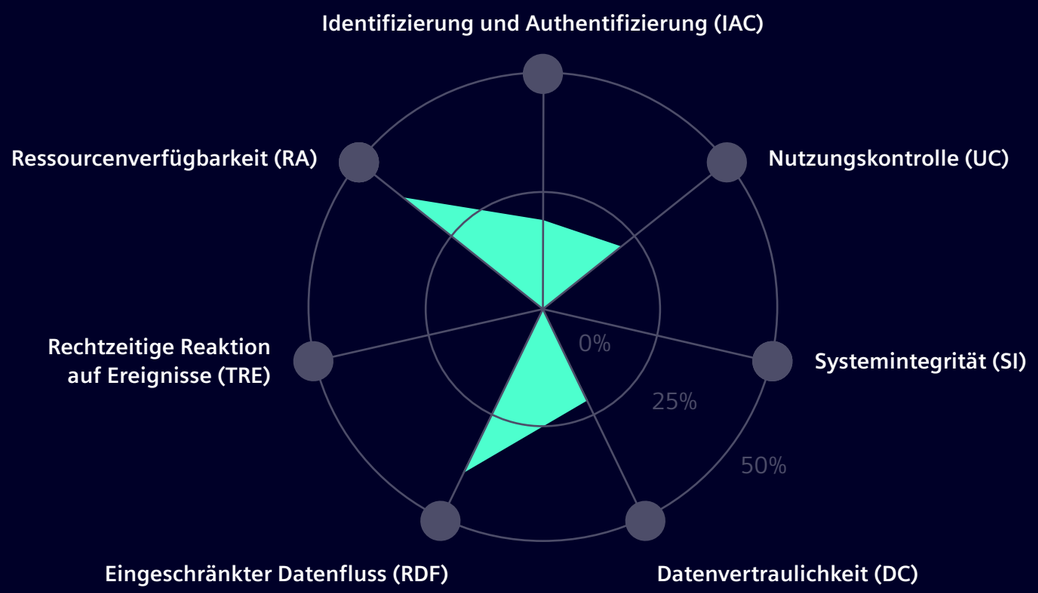
Risikobewertung

CRA-Bereitschaftsbewertung auf Grundlage einer Lückenanalyse gemäß IEC 62443

Beispielbericht

Prozentuale Erreichung des Sicherheitsziels (SL-T)

7 grundlegende Anforderungen



Ganzheitliche Analyse von Bedrohungen und Schwachstellen

Sicherheitsbewertungen umfassen eine gründliche Analyse von Bedrohungen und Schwachstellen, die Identifizierung von Risiken sowie Empfehlungen zur Schließung der ermittelten Lücken. Dadurch wird die Transparenz maximiert und Sie erhalten einen vollständigen Überblick über den aktuellen Sicherheitsstatus Ihrer Maschine(n).

Wir bieten eine gründliche Bewertung der Konformität mit IEC 62443 und CRA (IEC 62443/CRA-Bewertung), um Maschinenbauer bei der Einhaltung des Cyber Resilience Act zu unterstützen.

Bericht zur Einhaltung von Sicherheitsvorschriften

Maschinen- und Zonenkritikalität

Risikobewusstsein

Lücken gegenüber IEC 62443

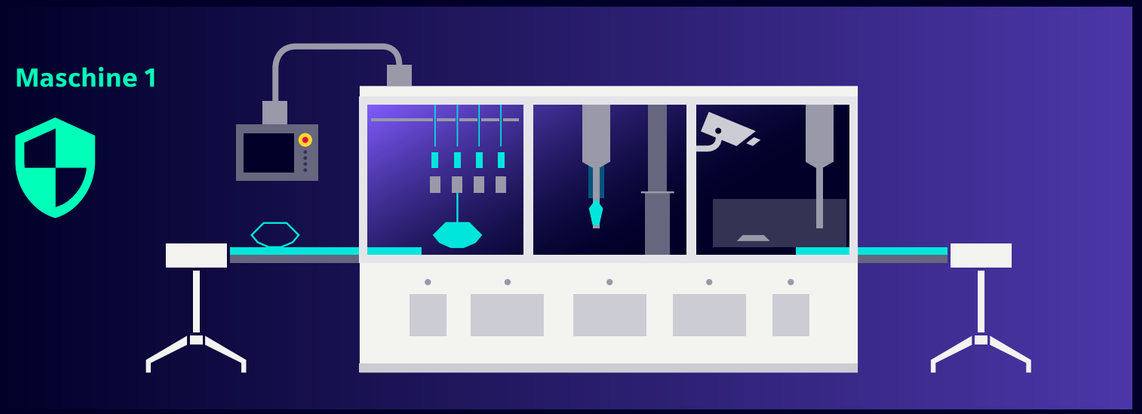
CRA-spezifische Antworten

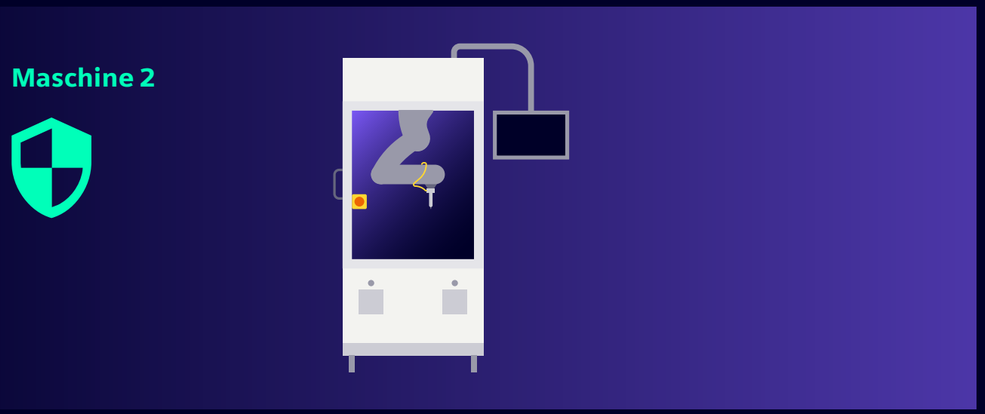
- Meldepflichten
- Schwachstellenmanagement

Der Weg zu mehr Sicherheit

- Konkrete Maßnahmen zur Verbesserung der Sicherheit
- Priorisierung nach Aufwand und Wirkung

Perimeter Protection
Firewall-basierte Kapselung





Kapselung – Einschränkung des Datenflusses

Schützen Sie das Maschinen-Subnetz, indem Sie den Datenfluss zu und von diesem Subnetz durch die Einführung einer SCALANCE S Firewall einschränken.

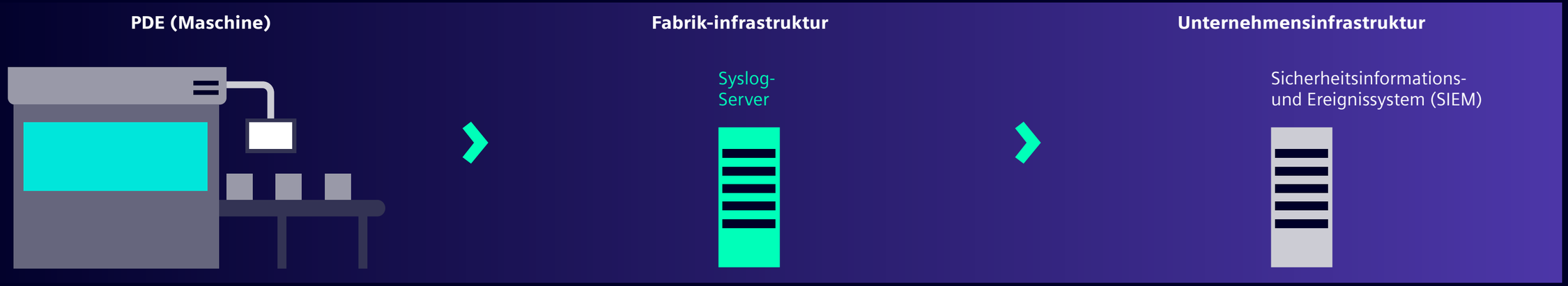
Laut CRA muss die Verfügbarkeit wesentlicher Funktionen durch die Implementierung oder Integration von Resilienz gegen Denial-of-Service-Angriffe (DOS) geschützt werden. Darüber hinaus muss die Angriffsfläche einschließlich externer Schnittstellen begrenzt und die Auswirkungen von Produkten auf andere Produkte oder Netzwerke verringert werden.

Die wichtigsten Punkte dieses Ansatzes sind:

- SCALANCE S Firewall zwischen der Maschine und anderen Netzwerksegmenten
- Schutz des Maschinennetzwerks und Begrenzung der Angriffsfläche
- Beschränkung des Datenflusses in das und aus dem Netzwerk

Event Logging

Wie man Ereignisse sicher überträgt, um Sicherheitsvorfälle zu erkennen



Weiterleitung von Sicherheitsereignissen mit dem in verschiedenen Produkten integrierten sicheren Syslog-Protokoll

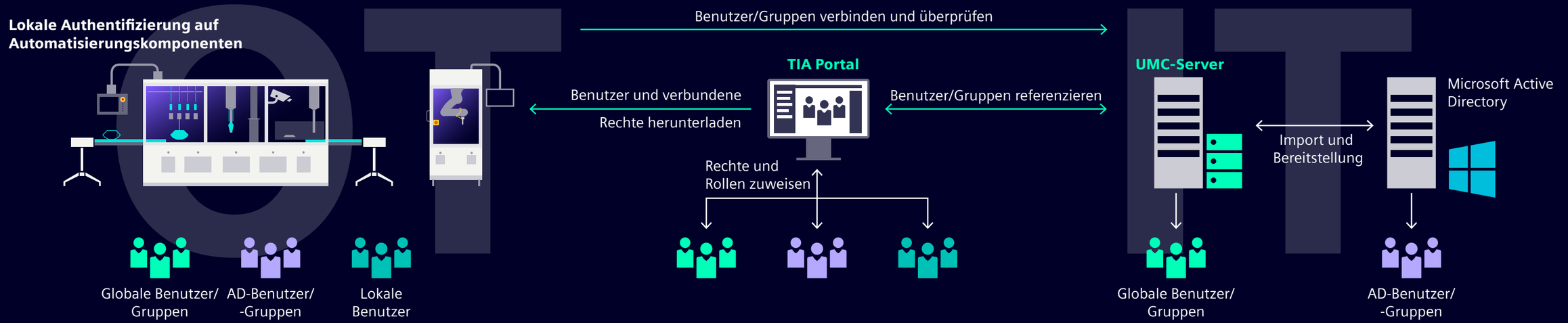
Die CRA verlangt die Meldung verschiedener Sicherheitsereignisse. Da das Maschinennetzwerk aus verschiedenen Komponenten besteht, ist ein zentrales Ereigniserfassungssystem für die Überwachung aller Ereignisse von Vorteil. Das Syslog-Protokoll ermöglicht die Weiterleitung von Ereignissen. SINUMERIK CNC und SIMATIC Steuerungen, SCALANCE Netzwerkkomponenten und SINAMICS Frequenzumrichter verfügen über eine integrierte Syslog-Client-Funktion, die eine benutzerfreundliche Lösung zur zentralen Erfassung von Ereignissen bietet.

Das Software-Tool SINEC INS (Infrastructure Network Services) für zentrale Netzwerkdienste mit integriertem Syslog-Server kann die Sicherheitsereignisse zentral erfassen. Es ermöglicht auch die Weiterleitung der Ereignisse an ein übergeordnetes SIEM-System.

Die wichtigsten Punkte dieses Ansatzes sind:

- Protokollierung von Sicherheitsereignissen
- Sicheres Senden von Ereignissen an einen zentralen Syslog-Server
- Weiterleitung von Ereignissen an ein SIEM-System

Authentication and Access Control
Mit zentralisierter Benutzerverwaltung



Herausforderung

- Die Konfiguration der Zugriffskontrolle für alle Systeme ist sehr aufwendig
- Die manuelle Konfiguration mehrerer Systeme ist eine sich wiederholende Aufgabe, bei der es leicht zu Fehlern kommen kann

Lösung

- Effiziente Benutzerverwaltung mit Benutzern und Gruppen auf OT-Ebene mit UMC Server und TIA Portal. Optionale Zuordnung von Benutzern und Gruppen aus Active Directory möglich.

Kundennutzen

- Effiziente Verwaltung der Benutzer für die gesamte Anlage
- Benutzer/Gruppen können aus einem bereits vorhandenen Microsoft AD-Server importiert werden, was Zeit und Aufwand spart
- Verbesserter Schutz durch personalisierten Zugriff anstelle von generischen Passwörtern

Access Control for Machines
Authentifizierung mit RFID

Eindeutige Identifizierung des Bedienpersonals an Maschinen und Anlagen, einschließlich:

- Zugangskontrolle
- Prüfpfad

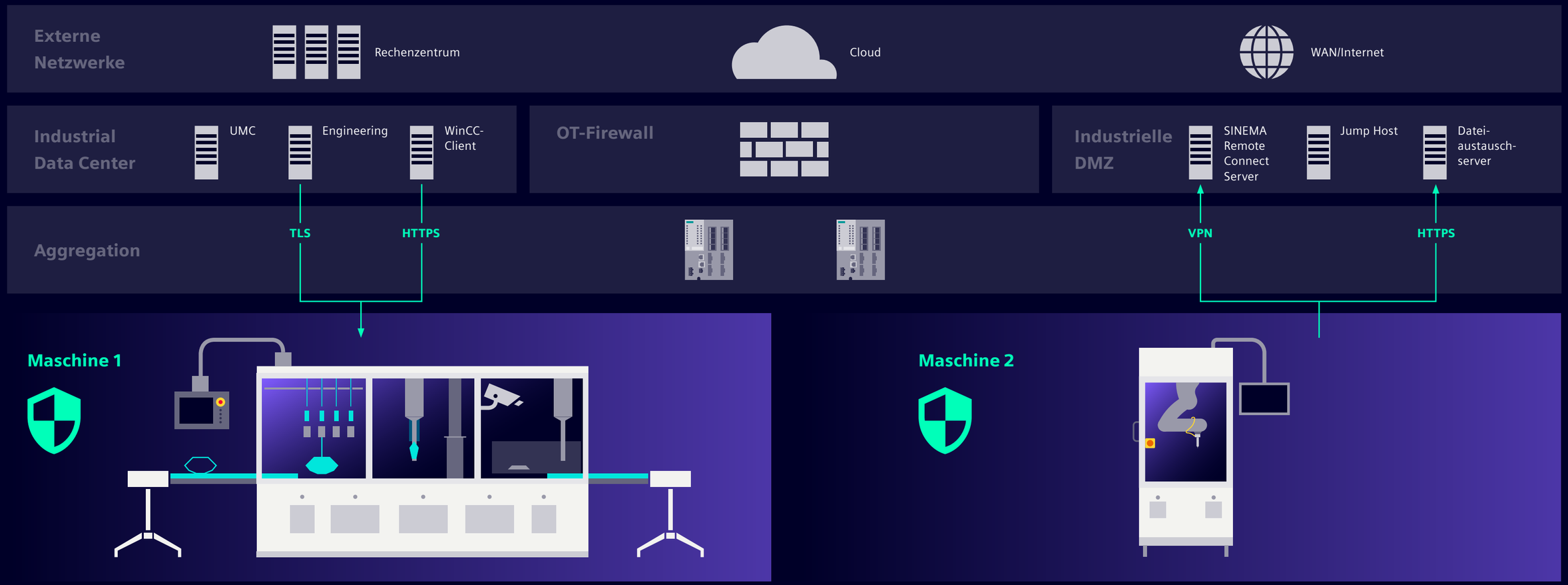
Sichere Zugangskontrolle und Zwei-Faktor-Authentifizierung

Der Zugangskontrollleser SIMATIC RF1000 unterstützt einmalige und permanente Anmeldungen mit RFID-Karte sowie Anmeldungen mit RFID-Karte einschließlich Benutzeranmeldedaten:

- Einmaliges Lesen der ID-Karte
- Permanentes Lesen der ID-Karte
- Einmaliges Lesen der ID-Karte mit zusätzlicher benutzerspezifischer Passwortauthentifizierung

Integrity and Confidentiality

Zertifikatsbasierte Kommunikation mit sicheren Protokollen



Integrity and Confidentiality
Zertifikatsbasierte Kommunikation mit sicheren Protokollen

Schützen Sie die Vertraulichkeit von Daten durch die Verwendung sicherer Protokolle

Der Schutz der Datenintegrität und der Vertraulichkeit sind zwei Verpflichtungen von CRA. Da die Maschine in der Regel in ein größeres Automatisierungsnetzwerk integriert ist, muss auch die Kommunikation mit übergeordneten Systemen geschützt werden.

Verschlüsselte Protokolle können in verschiedenen Produkten verwendet werden:

- SIMATIC und SINUMERIK Steuerungen können Open User Communication auf Basis von TLS, HTTPS und verschlüsselten OPC-UA-Protokollen verwenden
- SCALANCE X Switches und SCALANCE S Firewalls unterstützen HTTPS für den Webserverzugriff
- Industrial Edge unterstützt verschiedene sichere Protokolle wie HTTPS, OPC UA und MQTT
- Der Zugriff auf WinCC Unified basiert auf HTTPS
- Darüber hinaus kann mit einer SCALANCE S Firewall ein VPN eingerichtet werden, um jedes andere Protokoll zu schützen

Die wichtigsten Punkte dieses Ansatzes sind:

- Verschlüsselung mit standardisierten Protokollen
- Unterstützung von PKI-Zertifikaten

Hardening

Härtung jeder Komponente zur Erhöhung des Schutzes und der Widerstandsfähigkeit

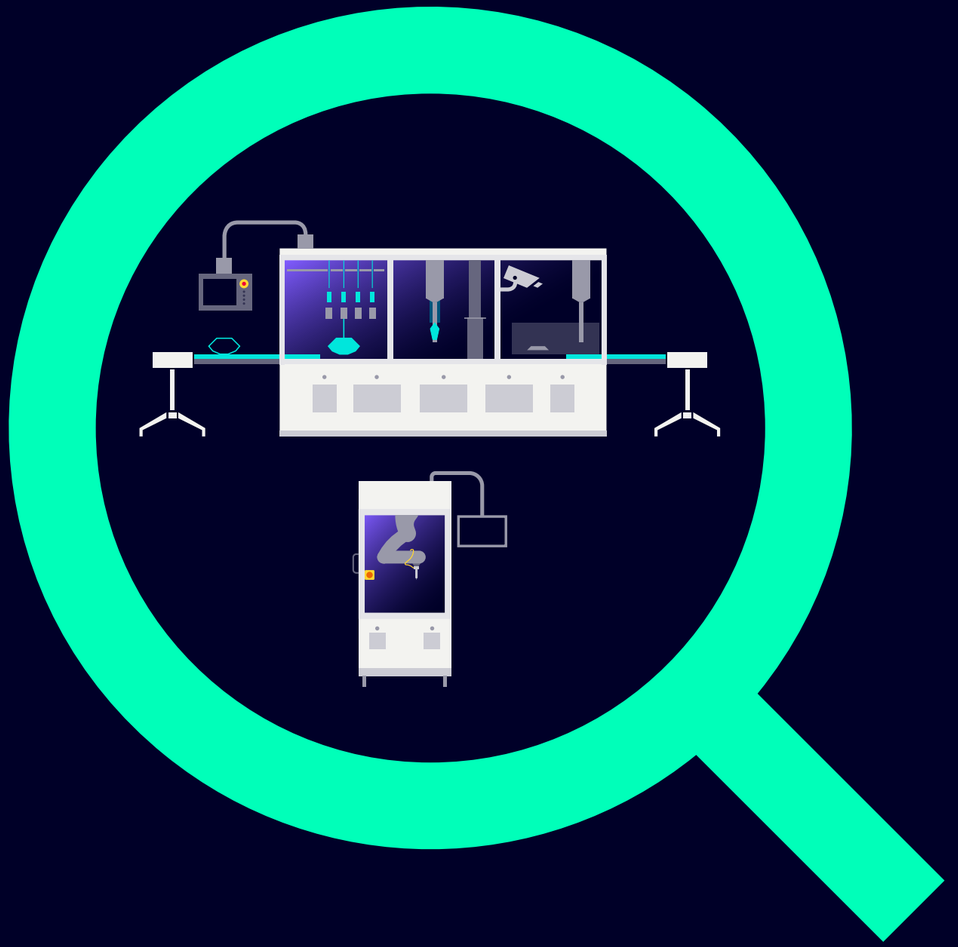
Angriffsflächen reduzieren

Die CRA verlangt die Reduzierung von Angriffsflächen, die Anwendung sicherer Konfigurationen und den Einsatz von Schutzmaßnahmen. Jede Komponente bietet verschiedene Sicherheitsfunktionen, die entsprechend konfiguriert werden müssen.

- Deaktivieren Sie nicht verwendete Dienste und Ports
- Sichern Sie die Anwendung mit Know-how-Schutz
- Führen Sie interne Überprüfungen der Gültigkeit von Daten, Programmen und Befehlen durch
- Verwenden Sie bei Bedarf eine zusätzliche Endpunktschutzlösung
- Überwachen Sie die Netzwerktopologie und geben Sie bei Änderungen Alarm aus
- Verwenden Sie zusätzliche fest verdrahtete Überwachungsmaßnahmen, z. B. für die Schranktür, um physische Manipulationen zu verhindern

Die wichtigsten Punkte dieses Ansatzes sind:

- Aktive Nutzung der integrierten Sicherheitsfunktionen jedes Produkts
- Verwendung von Diagnosedaten wie Topologie und Portstatus für die grundlegende Selbstüberwachung



Security Testing and Scanning

Die Maschine auf Schwachstellen scannen und eine Dokumentation erstellen

Regelmäßige Tests zur Dokumentation

Die CRA verlangt wirksame und regelmäßige Tests und Überprüfungen der Sicherheit von Produkten mit digitalen Elementen. Darüber hinaus müssen identifizierte Schwachstellen dokumentiert werden.

Mit SINEC Security Inspector können automatisierte Sicherheitstests einfach durchgeführt werden.

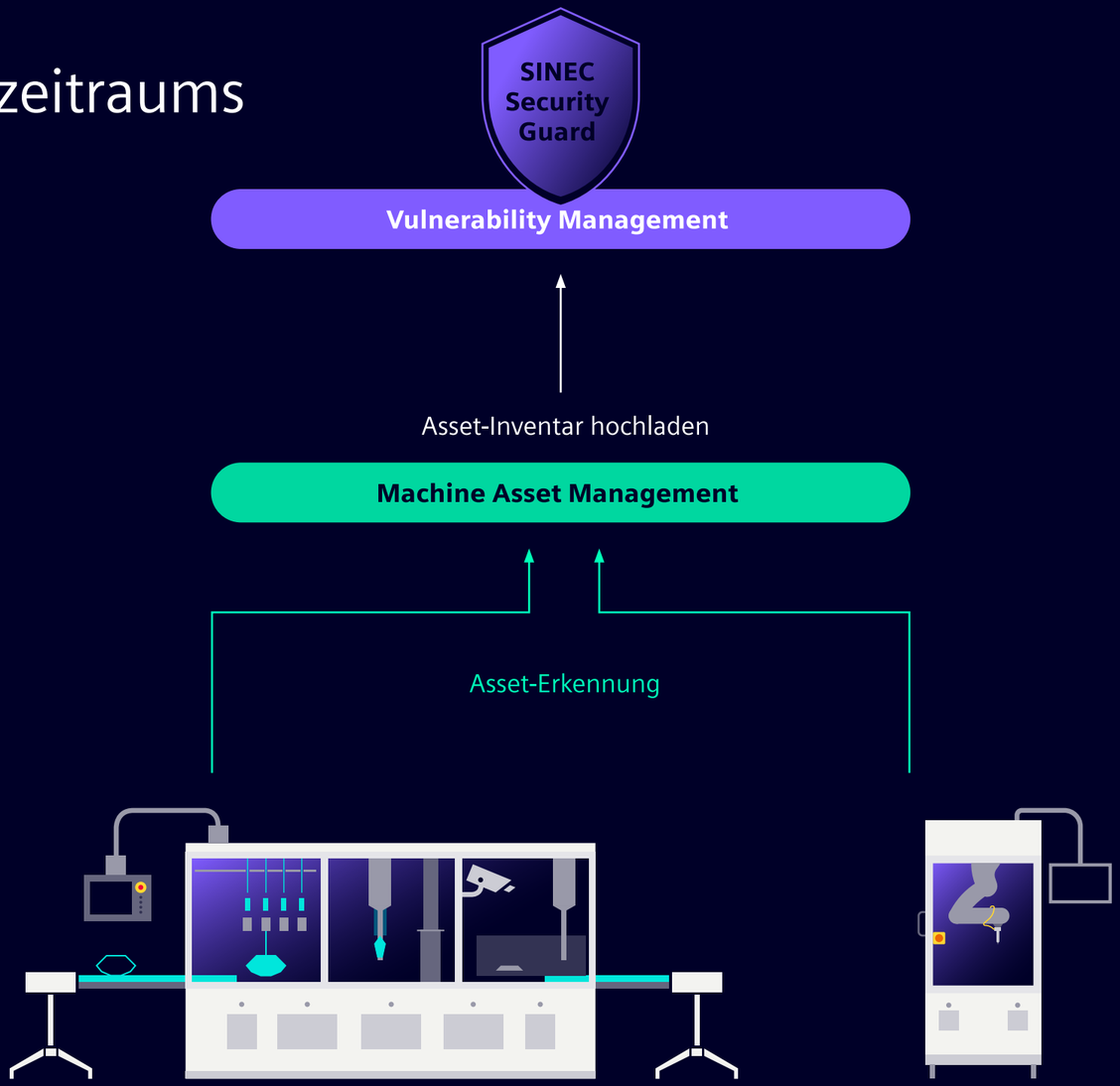
Die wichtigsten Punkte dieses Ansatzes sind:

- Eine intuitive, webbasierte Benutzeroberfläche mit assistentengestütztem Workflow
- Ein umfangreiches Toolset zur Verbesserung von Erkenntnissen, Compliance und Qualität wird durch vordefinierte Testfälle und unterstützte Testtools bereitgestellt
- Scan- und Testfälle wurden an die Anforderungen von OT-Netzwerken angepasst
- Auswahl verschiedener Sicherheitstests mit weitreichenden Funktionen zur Erkennung von Schwachstellen

Alternativ bietet Siemens einmalige Scan-Services an, um diese Sicherheitstests durchzuführen und einen Bericht zu erstellen.

Vulnerability Discovery and Management

Sichern Sie die Maschine während des Supportzeitraums



Identifizieren und dokumentieren Sie Schwachstellen

Mit einer cloudbasierten, automatisierten Lösung bleiben Sie über Schwachstellen in heterogenen Beständen digitaler Assets auf dem Laufenden.

Die CRA verlangt die Identifizierung und Dokumentation von Schwachstellen sowie die Bereitstellung von Updates für diese. Anstatt jede veröffentlichte Schwachstelle manuell mit der Asset-Liste abzugleichen, benachrichtigt SINEC Security Guard die Benutzer automatisch über relevante Schwachstellen, die ihre Assets betreffen. Dies reduziert den Aufwand für den Maschinenbauer erheblich und ermöglicht eine schnelle, strukturierte Benachrichtigung der Maschinenbesitzer.

- Abgleich des Maschinenbestands mit den Sicherheitshinweisen der Komponentenhersteller (BOM oder SBOM)
- Priorisierung der Schwachstellenrisiken auf der Grundlage der einzigartigen internen Architektur jeder Maschine
- Durch ein integriertes Aufgabenmanagement können Maßnahmen zur Risikominderung definiert und geplant oder an Workflow-Lösungen (z. B. ServiceNow®) weitergeleitet werden

Vulnerability Management Services

Bleiben Sie über Schwachstellen auf dem Laufenden und reagieren Sie umgehend

1. Einfaches Schwachstellenmanagement

Die Vilocify Vulnerability Service-Plattform bietet eine sichere und effiziente Lösung für die Schwachstellenanalyse. Über eine HTTPS-verschlüsselte Verbindung können Benutzer auf unser umfassendes Bewertungstool zugreifen. Die Plattform verfügt über eine intuitive Benutzeroberfläche, die den Prozess des Schwachstellenmanagements vereinfacht.

2. Ein Service für alle Komponenten

Er unterstützt alle Arten von Komponenten von Drittanbietern, von Open Source bis COTS, von Software bis Hardware, und bietet einen Überblick über die Schwachstellen in einem einzigen Service.

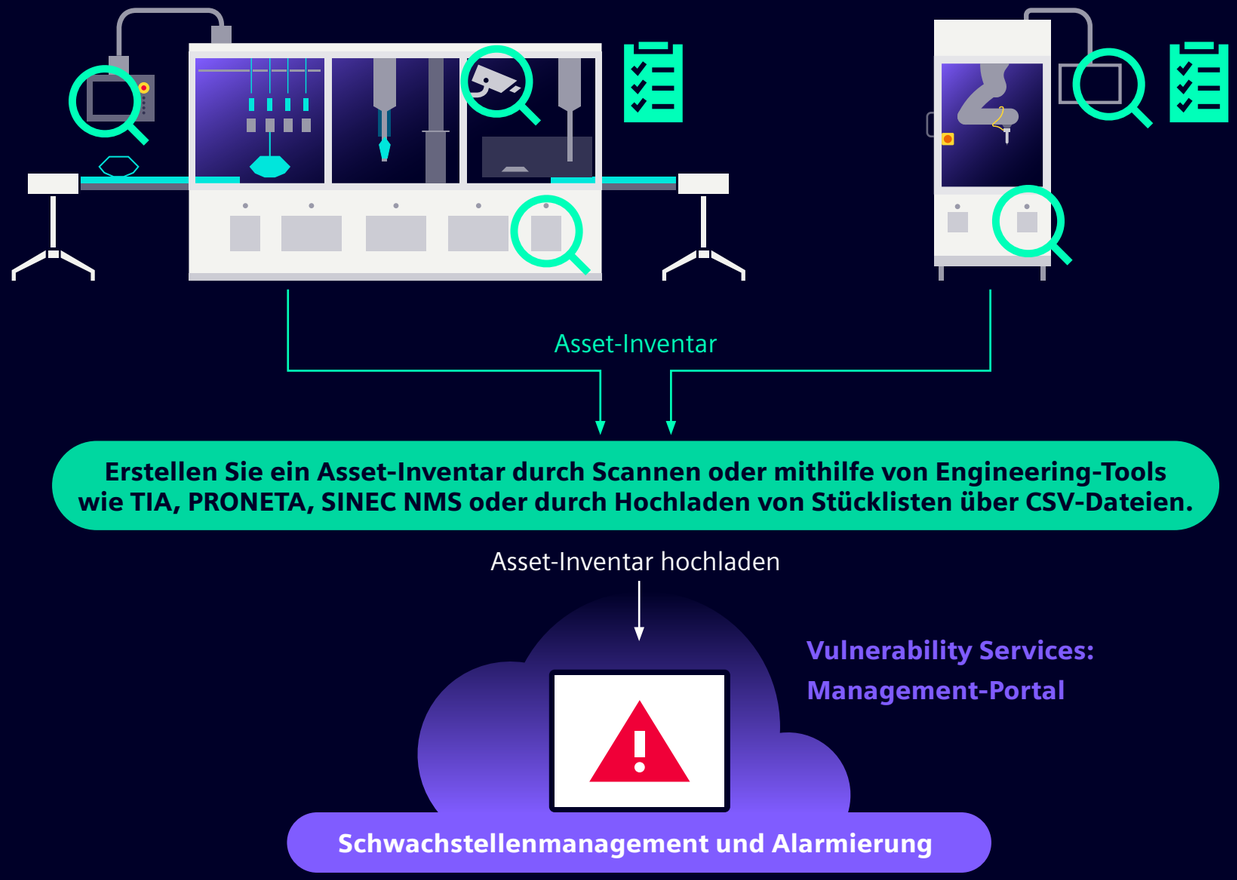
3. Transparente Informationen zum Lebenszyklus

Vulnerability Services halten Sie proaktiv über den offiziellen Support-Status auf dem Laufenden, einschließlich des Endes der Lebensdauer von Komponenten, sodass Sie Ihre Endkunden entsprechend informieren können.

1500
Quellen für Informationen über Schwachstellen

76%
schneller als Suchmaschinen

260k
Komponenten von Drittanbietern



Weitere Sicherheitsrichtlinien
Härtung von Siemens Produkten

Entdecken Sie mehr:

↗ Zusätzliche Informationen zu industriellen Security-Maßnahmen

↗ Security-Richtlinien für SIMATIC HMI Geräte

↗ Empfohlene Security-Einstellungen für IPCs in der industriellen Umgebung

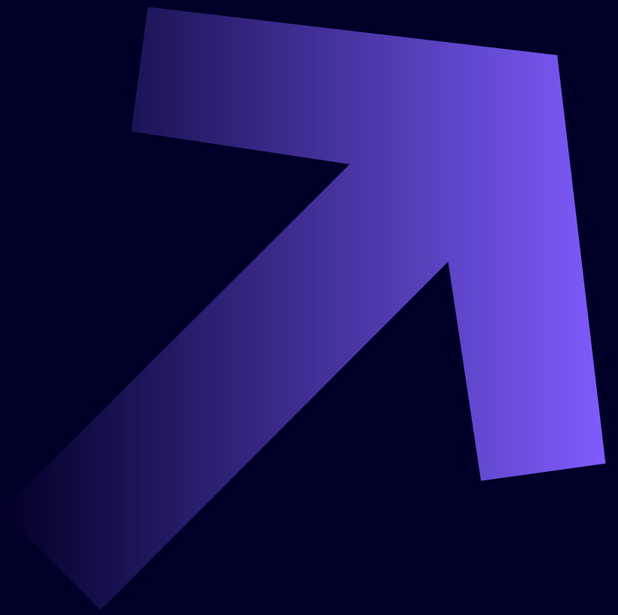
↗ Security mit SIMATIC S7 Steuerungen

↗ SIMATIC Prozessleitsystem PCS 7 Sicherheitskonzept (Grundlagen)

↗ SIMATIC Prozessleitsystem PCS 7 Kompendium Teil F – Industrial Security

↗ SINUMERIK ONE Dokumentation

↗ Weitere Informationen zu Vulnerability Services



Sprechen wir über OT-Sicherheit. Vernetzen wir die Experten.

Handeln wir gemeinsam. Jetzt!

Kontakt

Herausgeber

Siemens AG
Digital Industries
Factory Automation
Postfach 4848
90026 Nürnberg
Deutschland