# WAGO Security Consulting

WAGO setzt auf ganzheitliches Sicherheitskonzept.

# Inhalt




Kontaktieren Sie unsere Experten
und lassen Sie sich beraten:
**cybersecurity@wago.com**

# Höchste Sicherheit für OT-Netzwerke

Die fortschreitende Digitalisierung in der heutigen vernetzten Welt bietet nicht nur Chancen, sondern auch erhebliche Risiken durch wachsende Angriffsflächen für Cyberkriminelle. Angesichts steigender Schäden durch Cyberangriffe und neuer EU-Richtlinien wie dem „Cyber Resilience Act" (CRA) und der „Network and Information Security Device 2" (NIS-2-Direktive) wird ganzheitliche Cybersecurity für Unternehmen unverzichtbar.

WAGO begegnet diesen Herausforderungen mit einem ganzheitlichen Sicherheitskonzept und bietet Beratungsdienstleistungen im Bereich OT-Security an, die durch eine Kombination aus passgenauen Hard- und Softwarelösungen ergänzt werden. Auf diese Weise helfen wir unseren Kunden dabei, ihre OT-Netzwerke zu stärken und bieten Anwendern dadurch ein erhöhtes Maß an Sicherheit.

## Gegenwart

**Neue Technologien** bringen **neue Risiken** mit sich. → **Mehr Cyberangriffe durch digitale Produkte**

**8,15 Billionen USD**
Schaden wurde 2023 weltweit durch Cyberangriffe verursacht.

**Kunden**
Opfer von Sicherheitslücken in digitalen Produkten

**Unternehmen**
Gewährleistung sicherer digitaler Produkte in der Lieferkette

### EU-Cybersecuritystrategie

**Erhöhung der Sicherheit** von wichtigen Diensten und vernetzten Geräten

Stärkung der **kollektiven Fähigkeiten** zur Reaktion auf größere Cyberangriffe

Weltweite Kooperationen zur Wahrung von **Sicherheit** und **Stabilität** im Cyberspace

# Zukunft

**Anzahl der mit dem IoT verbundenen Geräte**

| 2023 | | 2030 |
|---|---|---|
| 15.9 Mrd. | 200 % | 32.1 Mrd. |

Die **Kosten** der durchschnittlichen **Ransomware-Angriffe** haben sich **nahezu verdoppelt** …

| 2023 | | 2030 |
|---|---|---|
| 812.380 USD | 90 % | 1,54 Millionen USD |

Quellenangabe:
www.statista.com
www.varonis.com
assets.sophos.com

# NIS-2-Direktive

## Neue EU-Richtlinie zur Stärkung der Cybersecurity

Um die digitale Infrastruktur nachhaltig zu verbessern, hat die Europäische Kommission neue Richtlinien zur Stärkung der Cybersecurity eingeführt, darunter die NIS-2-Richtlinie (Network and Information Security Directive). Diese erweitert die Vorschriften der ursprünglichen NIS-Richtlinie und verpflichtet Unternehmen je nach Kategorie und Branche zu einem effektiven Risikomanagement, um den Betrieb ihrer digitalen Infrastruktur und Dienstleistungen optimal zu schützen.

Ziel der NIS-2-Richtlinie ist es, die Resilienz kritischer Infrastrukturen gegen Cyberbedrohungen zu stärken, indem sie höhere Sicherheitsstandards, eine bessere Zusammenarbeit zwischen den Mitgliedsstaaten und Meldepflichten für Sicherheitsvorfälle vorschreibt. Sie betrifft zusätzliche Sektoren – darunter Energie, Verkehr, Industrie, Gebäude und digitale Dienstleistungen. WAGO ist ebenfalls von diesen Richtlinien betroffen und passt sein Sicherheitskonzept an die komplexen Vorgaben an. Die nachfolgende Grafik veranschaulicht, wie WAGO Kunden hilft, die entsprechenden Anforderungen umzusetzen.

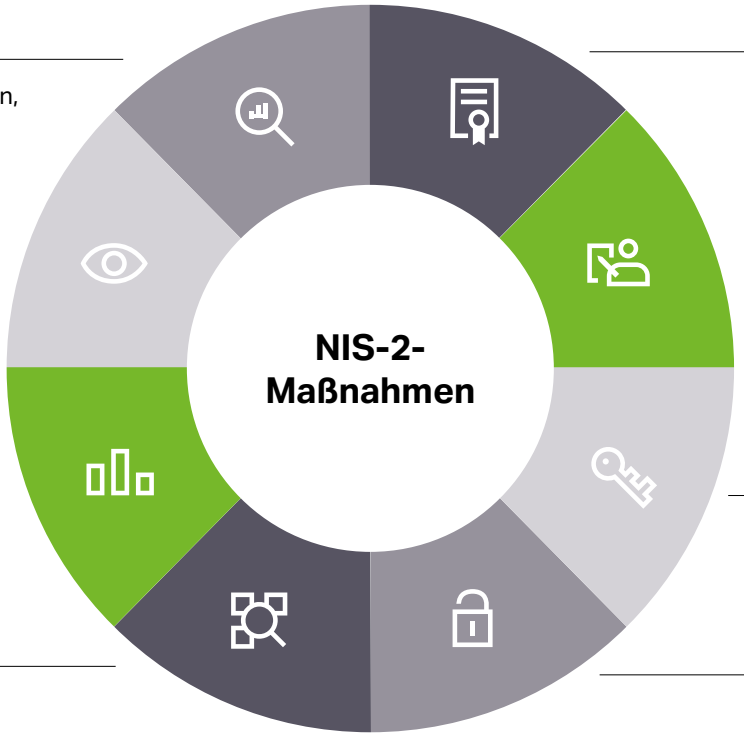
### Wie WAGO bei der Umsetzung der NIS-2-Richtlinie hilft

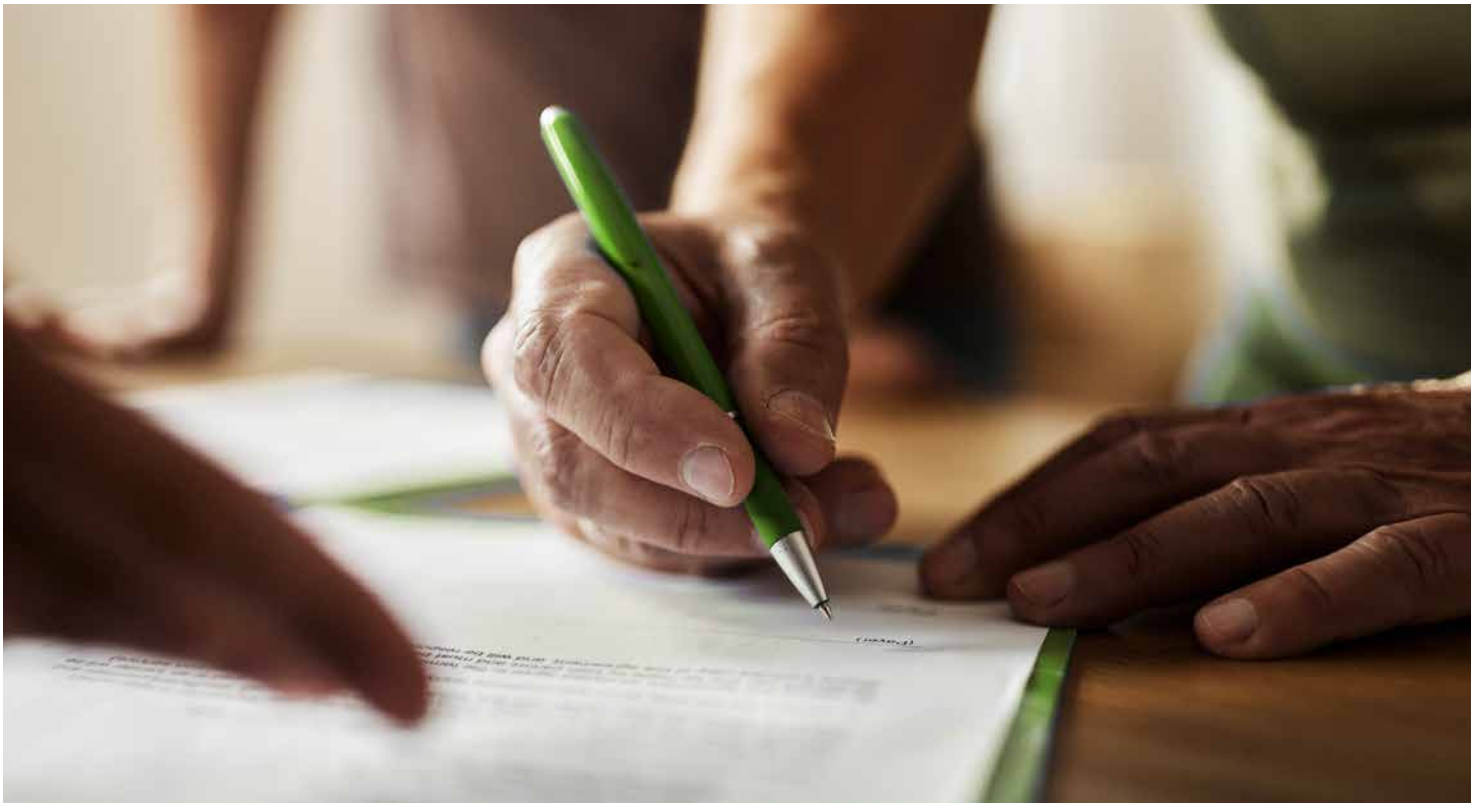
**1 Risikoanalyse**
- Kontinuierliche Risikobewertung zur Risikoidentifikation, Risikoanalyse und Risikobewertung
- NIS2-Exekutivbericht

**2 Beobachtung von Vorfällen**
- Kontinuierliche Überwachung der gesamten CPS-Umgebung
- OT-Alarm und Incident-Benachrichtigung an firmeninternes/externes SOC

**3 Geschäftskontinuität**
- Kontinuierliche OT-Bedrohungs- und Anomalieerkennung in Echtzeit
- Datengesteuerte Risikobewertung, Schwachstellenzuordnung und Empfehlungen zur Risikominderung

**4 Netzwerksicherheit**
- Echtzeit-Transparenz des OT-Netzwerks – fokussierte Kommunikation mit ICS-Geräten
- Überwachung von Verstößen gegen OT-Netzwerkrichtlinien
- Überwachung und Validierung des externen und gesicherten Remote-Zugriffs





## 5 Wirksamkeitsbewertung der Cybersecuritymaßnahmen

- Breach-Angriffsvektorsimulationen und „Was-wäre-wenn“-Szenarien
- Auf Sicherheitsrisiken basierende Bewertungsberechnungen
- Budget- und Aufwandsplanungstools

## 6 Grundlegende Cyberhygienepraktiken und Cybersecurityschulungen

- Breach-Angriffsvektorsimulationen und „Was-wäre-wenn“-Szenarien
- Die Ergebnisse der Risikobewertung enthalten vorrangige Empfehlungen für die wirksamsten Gegenmaßnahmen und den Schulungsbedarf

## 7 Integrität und Vertraulichkeit sensibler Betriebsdaten

- Verschlüsselungstechniken schützen sensible Informationen wie Steuerbefehle und Sensordaten vor unbefugtem Zugriff und stellen sicher, dass nur autorisierte Benutzer auf diese Daten zugreifen und deren Integrität gewährleistet ist.

## 8 Personalwesen, Zugangskontrolle und Bestandsverwaltung

- Vollständige automatische Bestandserkennung und Inventarisierung
- Echtzeit-Überwachung für neue Kommunikations-, Ressourcen- und Netzwerkänderungen

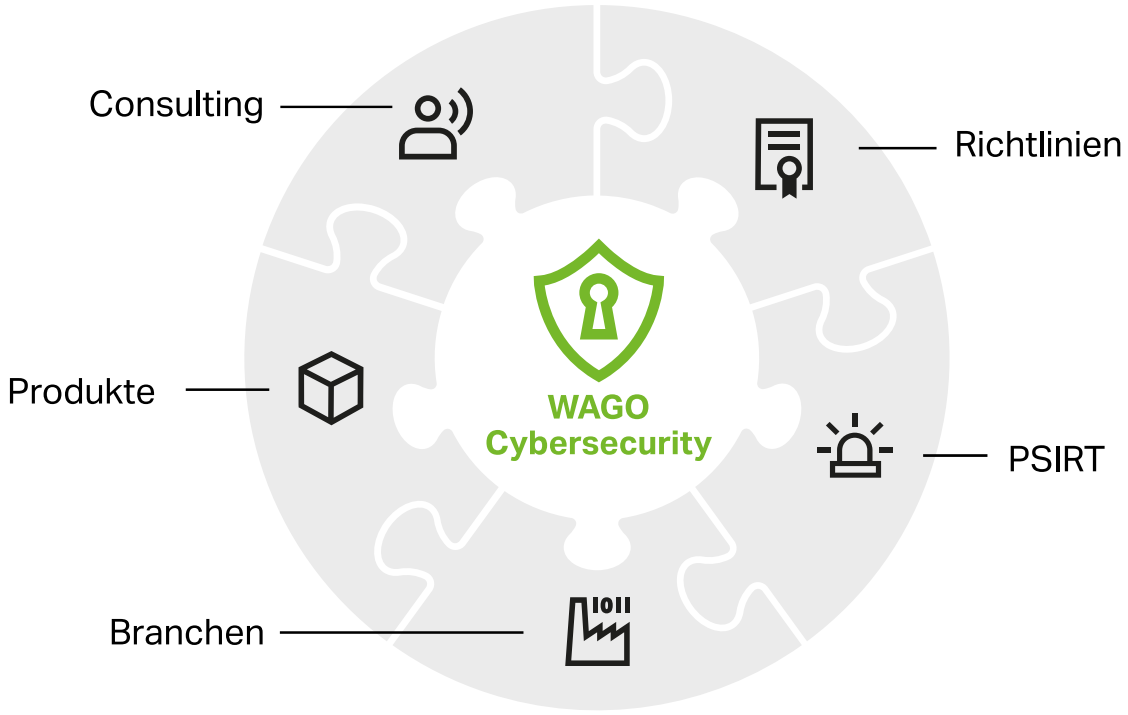
# Ganzheitliche Cybersecurity

## WAGO Cybersecurity Consulting für höchste Sicherheit

Cyberangriffe auf OT-Netzwerke, -Systeme und -Geräte können den Betrieb stören, die Sicherheit gefährden und zu erheblichen finanziellen Verlusten führen. Um potenziellen Bedrohungen entgegenzuwirken, müssen Unternehmen künftig beide Ebenen – sowohl OT als auch IT – in den Fokus nehmen und ein ganzheitliches Sicherheitskonzept implementieren. Neben den aktuellen Entwicklungsprozessen gemäß der Norm IEC 62443 erweitert WAGO daher sein Angebot um den Bereich Cybersecurity Consulting, um Anwendern maximale Sicherheit zu gewährleisten.

Dank dieses Rundumblicks über alle Ebenen hinweg unterstützt WAGO Unternehmen maßgeblich dabei, die anspruchsvolle NIS-2-Richtlinie und weitere Konformitätsprojekte zu erfüllen. Ein weiterer Pluspunkt: Zudem sind die Sicherheitslösungen auf die individuellen Bedürfnisse spezieller Märkte wie Smart Factory, Smart Building oder auch Smart Energy zugeschnitten.

Weitere Informationen unter **wago.com/cybersecurity**


Consulting
Richtlinien
Produkte
WAGO
Cybersecurity
PSIRT
Branchen

# Das WAGO Security Consulting umfasst fünf Bereiche:

## WAGO Security Consulting

### Evaluate

**Security Assessments und Audits**
Wir analysieren den aktuellen Sicherheitsstatus Ihrer OT-Systeme durch umfassende Assessments und Audits. Dabei identifizieren wir Schwachstellen, Sicherheitslücken und potenzielle Risiken in bestehenden OT-Infrastrukturen und Prozessen, um eine fundierte Grundlage für weitere Maßnahmen zu schaffen. Darüber hinaus berücksichtigen wir rechtliche Anforderungen, um die Compliance sicherzustellen.

### Detect

**Anomalieerkennung**
Durch den Einsatz eines „Intrusion Detection Systems" überwachen wir kontinuierlich Ihre OT-Landschaft, um ungewöhnliche Aktivitäten frühzeitig zu erkennen. So können Bedrohungen proaktiv identifiziert und neutralisiert werden, bevor sie zu ernsthaften Sicherheitsvorfällen führen. Dabei achten wir stets darauf, regulatorische Vorgaben, einschließlich der NIS2-Richtlinie, zu erfüllen.

### Design

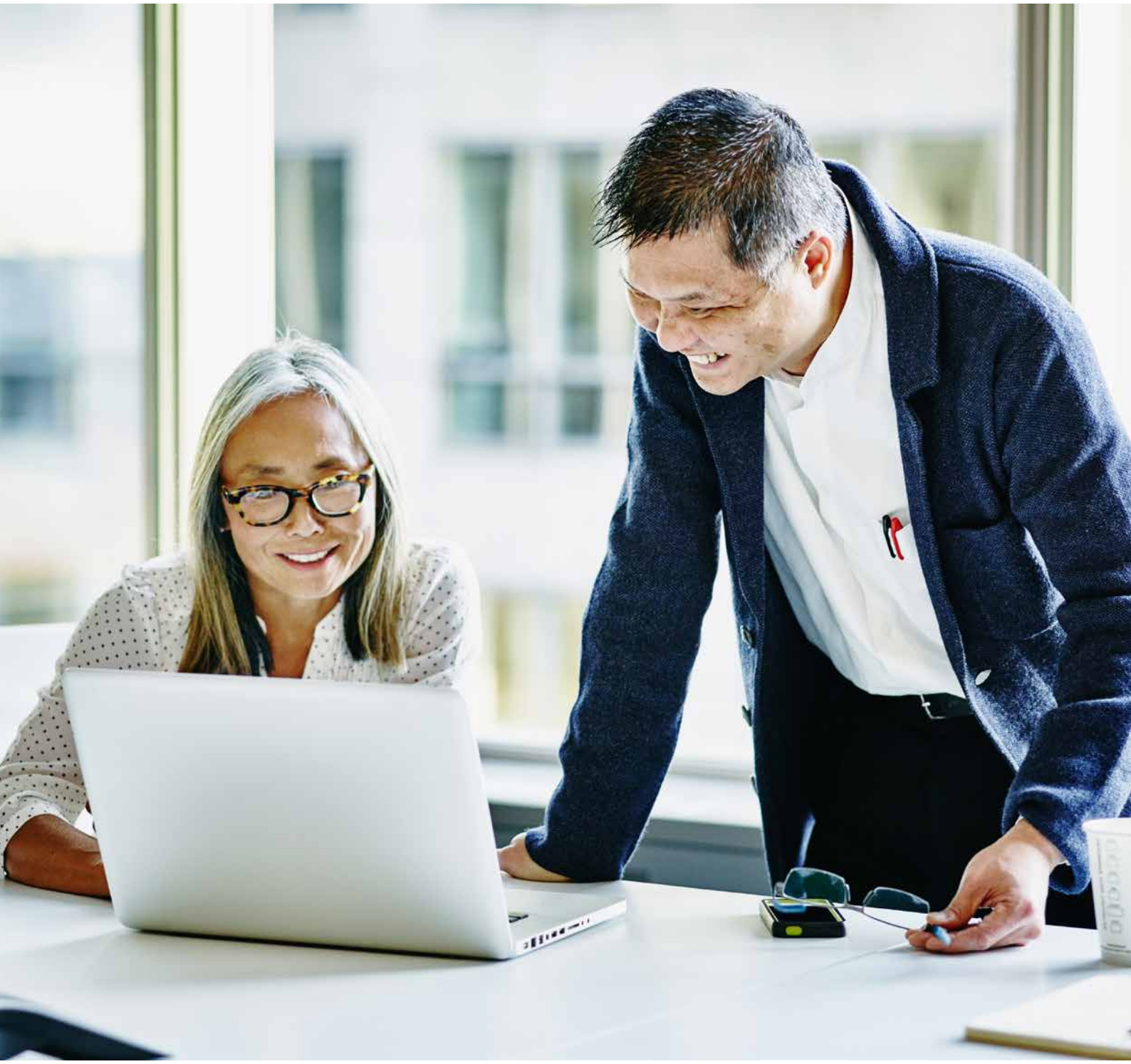
**Security Concept**
Auf Basis der gewonnenen Erkenntnisse entwickeln wir ein maßgeschneidertes Sicherheitskonzept, das den individuellen Anforderungen Ihrer OT-Umgebung gerecht wird. Wir definieren Richtlinien, Alarme und Maßnahmen, um heutigen und zukünftigen Bedrohungen vorzubeugen.

### Implement

**Technische Umsetzung**
Nach der Konzeption setzen wir die empfohlenen Sicherheitslösungen technisch in Ihrer OT-Umgebung um. Dies umfasst die Integration von Hard- und Softwarelösungen, um den Schutz Ihrer OT-Infrastruktur zu gewährleisten.

### Enable

**Insights und Awareness**
Wir bieten Cybersecuritypersonal einen übersichtlichen Einblick in die OT-Systeme ihres Unternehmens und stellen dafür umfangreich Berichte und Analysen zur Verfügung. So wird ermöglicht, dass effektive Maßnahmen zur Erhöhung der Sicherheit ausgewählt werden und das OT-Netzwerk gezielt gegen Angriffe optimiert wird.



# WAGO Cybersecurity Network Sight

## Netzwerksichtbarkeit und Anomalieerkennung

**Passive Überwachung kritischer Infrastruktur- und Industrienetzwerke auf Anomalien in Topologie sowie Verhalten und sofortige Erkennung von Cyberbedrohungen**

WAGO Cybersecurity Network Sight konsolidiert die Sichtbarkeit in der gesamten OT-Umgebung und verbessert die Sicherheitslage sowie die Einhaltung neuer Cybervorschriften und -richtlinien.

**Automatisches Erkennung**
Erfassung von Netzwerktopologien und Generierung von Verhaltensmodellen

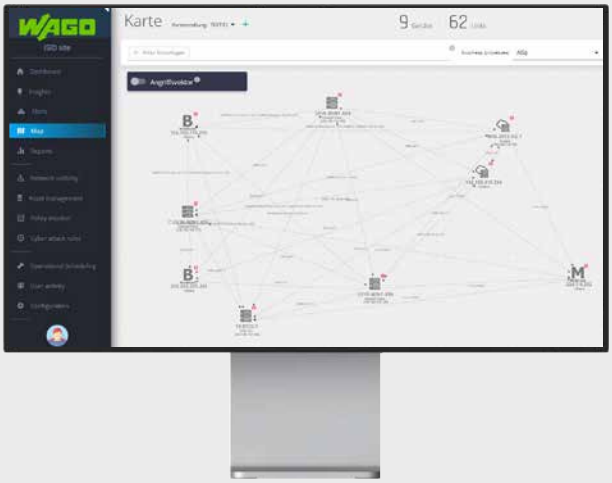
**Netzwerkanalyse**
DPI-basierte Analyse des Netzwerk-verkehrs ohne Unterbrechung des aktiven Betriebs

**Zentralisierte Netzwerküberwachung**
Überwachung von segmentierten Netzwerken in einer einzigen Anwendung durch den WAGO Cybersecurity Collector

**Konfigurationsüberwachung**
Kontinuierliche Überwachung der Konfiguration von beispielsweise Steuerungen und anderen Netzwerk-komponenten

**Alles auf einem Blick**
Kontrolle sämtlicher Installationen von Cybersecurity Network Sight durch Cybersecurity Management, unabhängig vom Standort oder Netzwerk

**Analyse des Angriffsvektors**
Präventive Erkennung von Schwachstellen und entsprechenden Angriffsvektoren in OT-Netzwerken




**Netzwerksichtbarkeit:** Durch passives Scannen des gesamten OT-Netzwerkverkehrs erstellt WAGO Cybersecurity Network Sight ein visuelles Netzwerkmodell für alle Geräte, Protokolle und Links.

## How it works

**Bestandsverwaltung:**
WAGO Cybersecurity Network Sight erkennt automatisch Assets und erstellt eine genaue Inventarisierung, die Rollen und deren Auswirkungen auf die OT-Umgebung enthält. Es überwacht Generationen von alten und modernen Asset-Typen sowie deren Kommunikationsprotokolle.

**Richtlinienüberwachung:**
Basierend aus der automatischen Erkennung erstellt WAGO Cybersecurity Network Sight gezielt Richtlinien für das Netzwerkverhalten, die individuell angepasst werden können. So ist es beispielsweise möglich, anwendungsspezifische Parameter oder Grenzwerte zu berücksichtigen.

**Schwachstellenmanagement:**
WAGO Cybersecurity Network Sight verfolgt kontinuierlich die neuesten Bedrohungsinformationen sowie SNORT-basierte Signaturen, gängige Angriffsmuster und Schwachstellen. Die präzise Identifizierung und Zuordnung bekannter Schwachstellen (CVE) trägt dazu bei, Industrieanlagen vor Cyberbedrohungen zu schützen. Das Asset-Patch-Management unterstützt Cybersecuritypersonal dabei, das System stets auf dem aktuellen Stand zu halten.

**Anomalieerkennung:**
WAGO Cybersecurity Network Sight erstellt ein Netzwerkmodell basierend auf dem Normalverhalten der Netzwerkteilnehmer und ermöglicht es so, Anomalien und potenzielle Angriffe zu erkennen.

**Betriebsverhalten:**
WAGO Cybersecurity Network Sight überwacht und prüft die Verwaltung von Geräten (SPS, RTU, IED) an Remote-Standorten und gibt Warnungen für Firmwareänderungen oder Konfigurationsänderungen wie Software-Updates oder das Ein- und Ausschalten von Edge Geräten aus. Außerdem protokolliert WAGO Cybersecurity Network Sight die Aktivität.

**Verhalten im Angriff:**
Die Software befasst sich mit bekannten Bedrohungen des Netzwerks, einschließlich solcher für PLC, Edge Devices und industrielle Protokolle, basierend auf Daten, die aus der gesamten Cybersecurityforschung gesammelt wurden.

**Alert-Management:**
Alerts, die beispielsweise bei der Erkennung von Anomalien ausgelöst werden, werden nach Typ und Schweregrad bewertet. Zusätzlich werden Assets in der Betriebsumgebung klassifiziert, um so False-Positives zu minimieren.

# Hardwareprodukte für WAGO Cybersecurity Network Sight

**Um die Hardwareanforderungen von WAGO Cybersecurity Network Sight für jede Netzwerkgröße zu bewältigen, können drei Hardwarekomponenten eingesetzt werden:**

**Edge Computer, Artikelnummer 0752-9800**

- für kleine Netzwerke

**Edge Computer, Artikelnummer 0752-9813**

- für mittelgroße Netzwerke, wie beispielsweise ganze Gebäude

**19-Zoll-Rack**

- für große Netzwerke, wie beispielsweise Produktionsanlagen

# WAGO Cybersecurity Analysis

Das datengesteuerte WAGO Cybersecurity Analysis unterstützt Sicherheitsteams, MSSP, Prüfer und Berater beim proaktiven Management von Cyberrisiken und beim Aufbau belastbarer Abläufe unter Einhaltung von Risikomanagementrichtlinien und -vorschriften wie NIS2, IEC 62443 und NIST CSF sowie branchenüblichen Best Practices.

**Angriffssimulation**
Bedrohungsintelligenzbasierte Simulationsszenarien für Angriffe auf das Netzwerk unter der Verwendung eines digitalen Zwillings

**Zonenspezifische Schlüsselindikatoren**
Bereichsspezifische Kennzahlen für Risiko-, Bedrohungs- und Kontrollniveaus

**ROI-optimierte Angriffsvektormitigation**
ROI-optimierter Minimierungsplan auf der Grundlage von Benutzerpräferenzen und Budget

**Durchführung**
Gezielter Maßnahmenplan zur effektiven Optimierung der Netzwerksicherheit

**Reporting**
Anpassbare Berichte für das Risiko- und Compliance-Auditing

**Einhaltung**
NIS2, IEC 62443, NIST CSF und Branchen-Best Practices


WAGO Cybersecurity Analysis unterstützt das Cybersecuritypersonal beim proaktiven Management von Risiken und dem Aufbau resilienter Betriebsprozesse. Außerdem unterstützt es bei der Einhaltung von Risikomanagementrichtlinien oder Normen wie NIS2, IEC 62443 und NIST CSF sowie branchenüblichen Best Practices.

## How it works

**Effektives Risikomanagement:**
WAGO Cybersecurity Analysis erkennt automatisch die wichtigsten Risikoindikatoren, bewertet den Zustand des Netzwerkes und ermittelt das entsprechende Risiko für einen erfolgreichen Angriff.

**Risikobewertungen:**
WAGO Cybersecurity Analysis bietet schnelle Risikobewertungen, wodurch beispielsweise die Zeit für Audits erheblich reduziert wird. Durch die automatische Erfassung relevanter Daten aus dem Netzwerk bewertet die Software Risiken präzise und ohne zusätzlichen Aufwand. So ist es möglich, die Sicherheit des Netzwerks zu jedem Zeitpunkt zu ermitteln.

**Optimierter Sicherheitsfahrplan:**
Der Risikoplaner unterstützt das Cybersecuritypersonal dabei, Ziele zur Risikominimierung, im Rahmen des Budgets, zu priorisieren. Dadurch ist es Anwendern möglich, die Maßnahmen zuerst umzusetzen, die den größten ROI im Rahmen der Cybersecurity bieten.

**Umgebungswissen:**
WAGO Cybersecurity Analysis stellt Berichte zu allen Netzwerksegmenten, Zonen, Verbindungen, Assets und Protokollen bereit. Wenn sich die Umgebung ändert, aktualisiert die Software automatisch seine Wissensdatenbank basierend auf aktuellen Daten.

**Lücken schließen:**
Die Ergebnisse der Risikobewertungen von WAGO Cybersecurity Analysis umfassen wichtige Kennzahlen für Risiko-, Bedrohungs- und Kontrollniveaus. Es erstellt einen umfassenden Härtungsplan, der den Anforderungen der ISA/IEC 62443 entspricht und nach Erreichung der Risikomanagementziele priorisiert ist. Best-Practice-Handbücher bieten Schritt-für-Schritt-Anleitungen, um Teams bei der Minderung von Schwachstellen, der Einhaltung von Vorschriften und der Gewährleistung operativer Resilienz zu unterstützen.

**NIS2 Compliance:**
Die NIS2-Richtlinie verlangt von betroffenen Unternehmen, Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen zum Management von Cybersecurityrisiken zu implementieren. WAGO Cybersecurity Analysis ist eine umfassende Lösung für das OT-Risikomanagement, welches bei der Einhaltung der NIS-2-Richtlinen unterstützt.

# WAGO Cybersecurity Management

## Netzwerküberwachung und Risikomanagement, zentralisiert für die gesamte OT-Infrastruktur

WAGO Cybersecurity Management dient als zentrale Managementplattform für die gesamte OT-Infrastruktur: Es konsolidiert die zuvor von WAGO Cybersecurity Network Sight gesammelten Daten sowie Alarme, ermöglicht eine zentrale Steuerung und gewährleistet eine koordinierte, effektive Reaktion auf Bedrohungen.

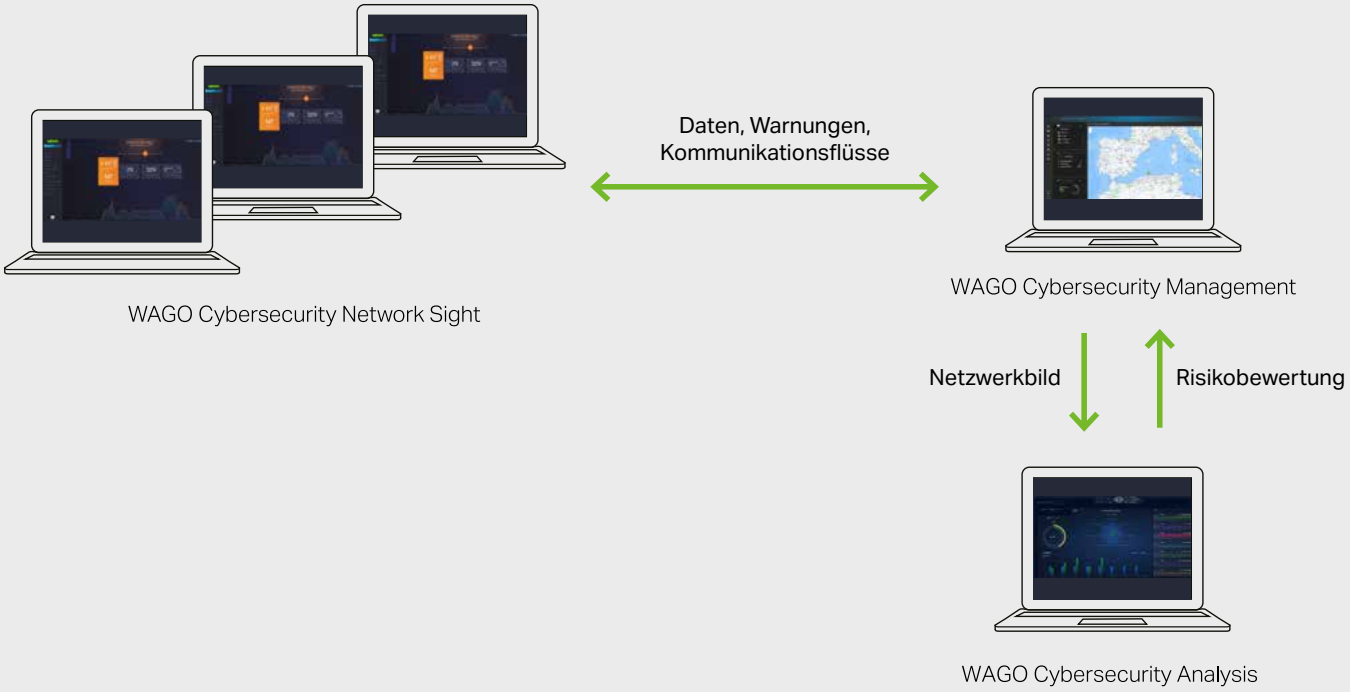
**Updates von Bedrohungsinformationen**
Bereitstellung von Bedrohungsinformationen und SNORT-Signaturen mit nur einem Klick für mehrere Instanzen des WAGO Cybersecurity Network Sight

**Zentrales Alert-Management**
Anzeige einer konsolidierten Ansicht aller Warnungen von allen Instanzen des WAGO Cybersecurity Network Sight

**Remote-Sicherung und -Wiederherstellung**
Über WAGO Cybersecurity Management können Anwender Back-ups einzelner Instanzen des WAGO Cybersecurity Network Sight planen und ggf. Daten wiederherstellen.

**Sichere Verbindungen**
Sämtliche Verbindung zum WAGO Cybersecurity Management sind gesichert und verschlüsselt. Außerdem unterstützt es eine einseitige Verbindung von zur Software, um die Segmentierung einzelner OT-Umgebungen zu gewährleisten.

**Benutzerverwaltung**
Benutzerverwaltung (Active Directory) mit Unterstützung für Benutzerrollen und Berechtigungen




## Automatisiertes, datengesteuertes Risikomanagement

Von seinem zentralen Standort (SOC, HQ, MSSP) aus überwacht und verwaltet das WAGO Cybersecurity Management die Datenerhebungstätigkeiten aller Instanzen des WAGO Cybersecurity Network Sight, bereichert und konsolidiert die Daten zentral. Es wandelt diese Daten in Netzwerk-Images sowohl pro Standort als auch firmenübergreifend um und bereitet sie automatisch für die Risikobewertung vor.
Datengesteuerte Risikobewertungen für einzelne Standorte und Unternehmen werden auf der Plattform WAGO Cybersecurity Analysis durchgeführt.

# WAGO Cybersecurity Collector

Kostengünstige, LAN-fähige Lösung zum Senden des Datenverkehrs verteilter Industrieeinheiten zum WAGO Cybersecurity Network Sight zur Analyse, ohne das Netzwerk zu belasten

**Aggregation und Tunneling**
Aufnehmen von Netzwerkdaten und sichere Übertragung an eine Instanz des WAGO Cybersecurity Network Sight

**Störungsfreier Betrieb**
Passives Scannen des Datenverkehrs in segmentierten Netzwerken

**Unidirektionale Übertragung**
Einseitige Übertragung des Netzwerkverkehrs

**Datenkomprimierung und -filterung**
Bis zu 1:10-Kompression des Verkehrs und Herausfiltern irrelevanter Daten

**Verschlüsseltes Tunneling**
Der gespiegelte OT-Verkehr wird über ein verschlüsseltes Tunnelprotokoll im Netzwerk übertragen.


## WAGO Cybersecurity Collector

### Technische Daten

Physischer Entwurf

**Montage:** Hutschiene/Wandhalterung
**Gehäuse:** Aluminium/Stahl, lüfterlos, IP30-bewertet
**Gewicht:** 500 g
**Abmessungen:** (mm; H x T x B) 110 x 90 x 30

**Hardware:**
CPU: Intel® Atom™ x5-E3940, 4-Core, 1,6 GHz
RAM: 8 GB LPDDR4
Massenspeicher: 64 GB

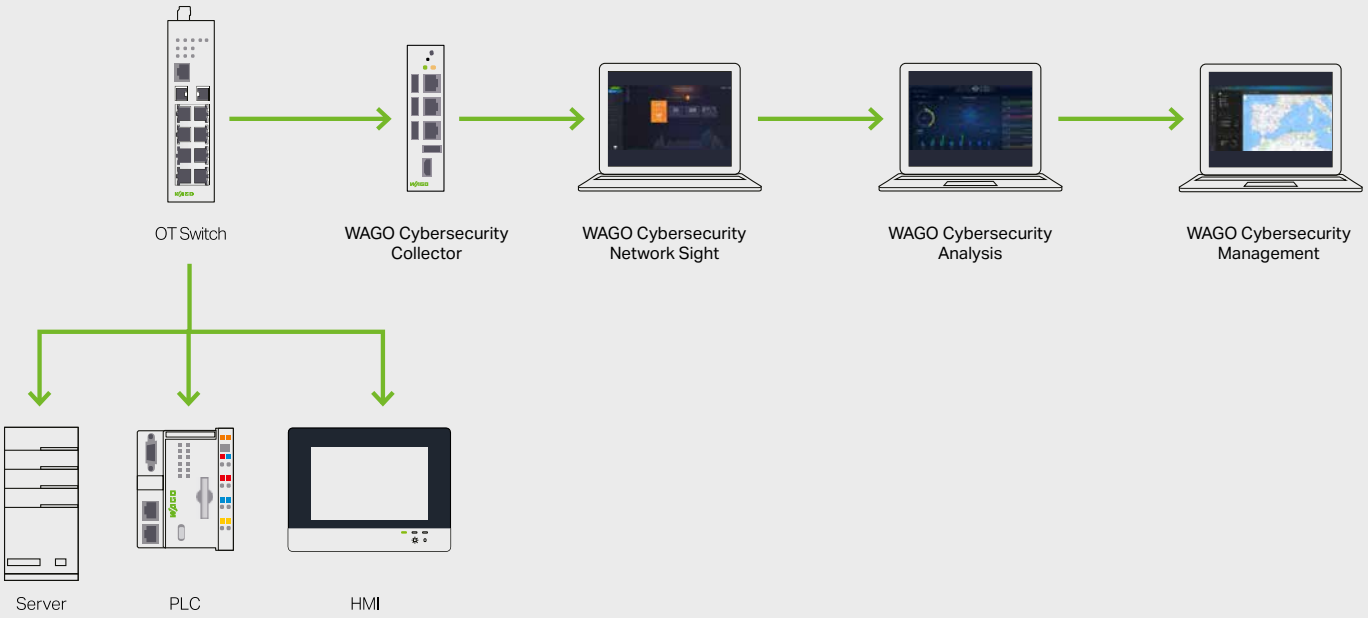
**Schnittstellen und Ports:**
3 x 10/100/1000BaseTX-Ports
RJ-45, RS-232 (TX/RX/GND)
RS-485, automatische Flusskontrolle
auf 8-poligem Klemmenblock
1 x USB 2.0
3 x USB 3.0
1 x Digitaleingang
1 x Digitalausgang
1 x HDMI-Anschluss

**Umgebungsparameter:**
Betriebstemperatur: -20 … 60 °C
Luftfeuchtigkeit bei Betrieb: 5 … 95 %
Zertifizierungen: CE, FCC, RoHS

**Stromversorgung:**
Stromversorgung (V DC): 12 … 24 V
Anschluss: 4-poliger Klemmenblock mit
Leistungsschalterfunktion

# Gemeinsam die Cybersecurity von morgen gestalten

Damit WAGO Cybersecurity Network Sight die bestmögliche Datenbasis bezieht, ist es optimal, die Software an einer zentralen Stelle im Netzwerk, wie einem Hauptswitch, zu platzieren. So wird gewährleistet, dass sämtliche Netzwerkteilnehmer überwacht werden können. Um auch Sichtbarkeit in segmentierte Bereiche des Netzwerkes zu bringen, ist es möglich, den WAGO Cybersecurity Collector in diesen Bereichen zu installieren. Dieser spiegelt die Netzwerkdaten des separierten Bereichs und sendet sie an WAGO Cybersecurity Network Sight. Die in WAGO Cybersecurity Network Sight zur Verfügung gestellten Daten können im Anschluss in nachgelagerten Systemen wie SOCs, SIEMs, Firewalls oder weiteren OT-Asset-Management-Systemen verwendet werden.




WAGO Cybersecurity Management und WAGO Cybersecurity Analysis ergänzen die Funktionalität von WAGO Cybersecurity Network Sight, um eine umfassende industrielle Sicherheitslösung zu schaffen. Hierbei dient das Management als zentrale Managementplattform, die mehrere Instanzen des WAGO Cybersecurity Network Sight in verschiedenen Standorten oder Segmenten des Netzwerks überwacht und verwaltet. Es konsolidiert die von WAGO Cybersecurity Network Sight gesammelten Sicherheitsdaten und Alarme, ermöglicht eine zentrale Steuerung und sorgt für eine koordinierte Reaktion auf Bedrohungen.

WAGO Cybersecurity Analysis hingegen führt simulationsbasierte Risikobewertungen durch und nutzt entweder die von WAGO Cybersecurity Network Sight oder Drittanbietern bereitgestellten Echtzeitdaten, um Schwachstellen und potenzielle Bedrohungen im OT-Netzwerk zu identifizieren. Diese Bewertungen unterstützen bei der Optimierung von Sicherheitsstrategien und helfen, proaktive Maßnahmen zur Bedrohungsprävention zu ergreifen. Zusammen bieten WAGO Cybersecurity Management und WAGO Cybersecurity Analysis eine strategische Erweiterung zu WAGO Cybersecurity Network Sight, die nicht nur die Überwachung und Erkennung, sondern auch die Verwaltung und Risikobewertung abdeckt.

**WAGO GmbH & Co. KG**
Postfach 2880 · 32385 Minden
Hansastraße 27 · 32423 Minden
**info@wago.com**
**www.wago.com**

| | |
|---|---|
| Zentrale | 0571/ 887 - 0 |
| Vertrieb | 0571/ 887 - 44 222 |
| Auftragsservice | 0571/ 887 - 44 333 |



MM-514117 - WAGO Security Consulting - 10/2024 - Printed in Germany - Änderungen vorbehalten