



CYBERSECURITY

OT Security Services und Lösungen

Wir begleiten Sie auf dem Weg zur besseren Absicherung Ihrer OT Umgebung, wir reduzieren die Komplexität und Ihre Aufwände, während Sie sich auf Ihre Kernaufgaben fokussieren

Dank der Digitalisierung wächst die Effizienz von Produktions- und Steuerungssystemen, da die direkte Kommunikation zwischen den Systemen vorangetrieben wird. Heute noch autarke industrielle Produktions- und Steuerungssysteme werden entlang der Supply Chain mehr und mehr vernetzt. Das führt zu Kostenreduktionen und Wettbewerbsvorteilen.

Jedoch werden die OT Systeme damit auch der Bedrohung durch Cyber Angriffe ausgesetzt. OT Industrienetzwerke und ICS-Komponenten sind verstärkt im Fokus der Angreifer, da diese von Haus aus schlechter geschützt sind, als IT- Systeme.

Aus eigener Erfahrung sind wir von Airbus CyberSecurity überzeugt, dass eine effiziente Produktion und ein innovatives Arbeiten nur in einer sicheren Umgebung vorstattgehen können. Für eine bessere Absicherung von kritischen Infrastrukturen und Industrieanlagen bieten wir Ihnen verschiedene, modulare Services und Lösungen an, die sich in unserem eigenen Haus bewährt haben.

Wir unterteilen diese Lösungen in drei Bereiche:



- **Analyze:** Erarbeitung von konkreten OT Security Maßnahmenempfehlungen für Ihre Anforderungen auf Basis einer effizienten Schwachstellen- und Risikoanalyse
- **Protect:** Entwicklung und Implementierung eines für Sie zugeschnittenen OT Cyber Security Konzepts
- **Manage:** Kontinuierliche Überwachung und Aktualisierung Ihrer Sicherheitsmaßnahmen durch unsere Managed Security Services

AIRBUS

Unsere OT Cyber Security Services und Lösungen im Überblick:

Phase	Serviceangebot	Leistungsinhalte
Analyse	OT Asset Discovery & Analysis	<ul style="list-style-type: none"> • Passive, technische Erfassung und Analyse der industriellen Netzwerke ✓ Überblick über die Komponenten im Produktionsnetzwerk und deren Kommunikation untereinander ✓ Identifizierung von Anomalien und Schwachstellen ✓ Schaffung einer Datenbasis für umfassende Risikoanalyse und Maturity Check
	OT Security Maturity Check	<ul style="list-style-type: none"> • Kompakter Überblick des Sicherheitsniveaus Ihrer Produktionssysteme ✓ Verständnis über den aktuellen Reifegrad, nach Best-Practice und ausgewählten Standards wie IEC 62443 ✓ Schaffung einer Datenbasis für Risikoanalyse ✓ Identifizierung priorisierter Handlungsfelder
	OT Security Pentesting	<ul style="list-style-type: none"> • Schwachstellen Analyse und aktive Security Tests Ihrer industriellen Netzwerke (wo möglich im OT Umfeld) ✓ Erhöhung des Bewusstseins für den aktuellen Stand der Absicherung ✓ Erlangung des Verständnisses für existierende Schwachstellen ✓ Verifikation der implementierten Maßnahmen
	OT Security Risk Assessment	<ul style="list-style-type: none"> • Ganzheitliche Risikobewertungen der industriellen Systeme unter Betrachtung der Eintrittswahrscheinlichkeit von Bedrohungen und möglichen Auswirkungen auf kritische Geschäftsprozesse ✓ Umfassende Risikobewertung mit Analyse der Auswirkung auf die Produktion und den Geschäftsbetrieb ✓ Vorschläge zur Risikoreduzierung bzw. Behandlung basierend auf der Priorisierung der identifizierten Risiken ✓ Erhalt einer Entscheidungsgrundlage zur Umsetzung von Maßnahmen
Protect	OT Security Design	<ul style="list-style-type: none"> • Ausarbeitung eines ganzheitlichen Cyber Security Konzepts, typische Fokusbereiche: <ul style="list-style-type: none"> - Absicherung und Segmentierung industrieller Netzwerke - Absicherung Endgeräte, Monitoring Design - OT Cyber Security Technologieevaluierung (Scouting) ✓ Security Konzepterstellung basierend auf Ihren kundenspezifischen Anforderungen, unserer industriespezifischen Expertise, „Best Practices“ und nationalen/internationalen Standards
	OT Security Integration	<ul style="list-style-type: none"> • Implementierung von OT Security Konzepten, typische Fokusbereiche sind: <ul style="list-style-type: none"> - Durchführung eines „Proof of Concepts“ mit evtl. Evaluierung 3rd Party Technologien - Konfiguration, Integration, Test und Validierung - Betriebshandbuch & Schulungen ✓ Schlüsselartig implementiertes Konzept für den OT Bereich durch erfahrene Experten mit aktuellem Spezialwissen über Sicherheitskonzepte und Technologien
	OT Security Training	<ul style="list-style-type: none"> • Schulungen für die Etablierung einer Sicherheitsorganisation und zur Erhöhung von Cyber Security Kenntnissen, typische Fokusbereiche sind: <ul style="list-style-type: none"> - Awareness Trainings - CyberRange und War Game Trainings - Vorträge und Live Hacking ✓ Kenntnisse und Gesamtverständnis der Security Bedrohungen und möglichen Lösungsansätzen
Manage	SOC4OT	<ul style="list-style-type: none"> • Managed Service für Konzepterstellung, Planung, Implementierung und Betrieb einer OT Security Monitoring Lösung ✓ Ganzheitliche Lösung zur Cyber Security Absicherung der OT Infrastruktur ✓ Kontinuierliche Anpassung der Lösung auf neue Sicherheitsanforderungen ✓ Langfristig kalkulierbare Kosten bei reduziertem Aufwand
	OT Secure Remote Management	<ul style="list-style-type: none"> • Managed Service für Anschaffung, Installation & Betrieb der Fernwartungsinfrastruktur Ihrer Systeme (inkl. Zugriffsprotokollierung, Verfügbarkeitsüberwachung & Reporting). Optional mit Security Monitoring ✓ Absicherung auf Stand der (europäischen) Technik entsprechend BSI Anforderung / Empfehlung BSI CS 108 ✓ Lokale Kontrolle durch Produktionspersonal ohne IT-Kenntnisse ausreichend, kein Spezialwissen erforderlich ✓ Kosteneinsparungen durch einheitlichen Service für alle Produktionssysteme

Was zeichnet uns aus:

- Langjährige Erfahrung bei der Umsetzung und beim Betrieb von Sicherheitskonzepten in sensiblen Bereichen mit agnostischem Ansatz nach Best Practices
- Branchenspezifisches Knowhow für kritische und komplexe Infrastrukturen und Produktionsumgebungen
- Ganzheitliche und integrierte Service- und Technologielösungen von Airbus und Airbus Partnern, flexibel anpassbar auf Ihre Anforderungen

Unsere Angebote sind modular aufgebaut und lassen sich ideal in bereits bestehende Kampagnen und laufende Maßnahmen integrieren. Gerne unterstützen wir Sie auch bei der Entwicklung neuer Kampagnen und Konzepte. Für weitere Informationen, sprechen Sie uns einfach an.

AIRBUS

Dieses Dokument ist nicht verbindlich. Änderungen vorbehalten. © 2018 Airbus CyberSecurity. Airbus, das Logo und die Produktnamen sind eingetragene Marken. Alle Rechte vorbehalten.
1018 D 0694

Airbus CyberSecurity

Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com