Fraunhofer ACADEMY

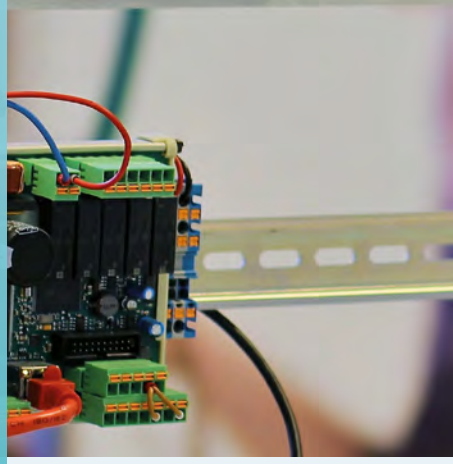
Weiterbildung im
Lernlabor Cybersicherheit

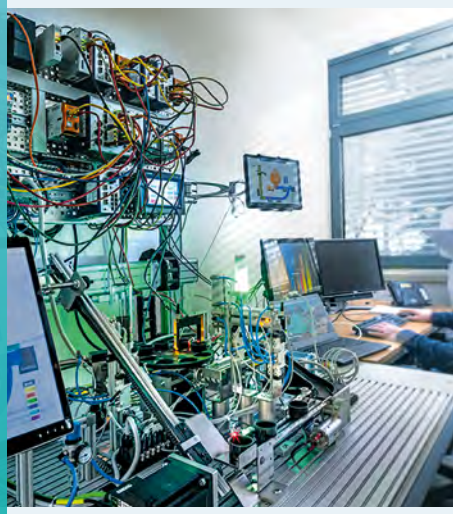
Know-how für mehr IT-Sicherheit

Industrielle Produktion

www.cybersicherheit.fraunhofer.de

Inhalt





1

2

3

Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy im Bereich Information und Kommunikation. Im Zentrum des umfassenden Angebots des Lernlabors stehen alle Themen rund um die IT-Sicherheit.

Impressionen aus unseren Lernlaboren Cybersicherheit:

1 Demonstrator für die Schulung: »Sichere Hardware- und Softwareplattformen für Industrieprodukte«.

2 Im Lernlabor Cybersicherheit für die industrielle Produktion wird moderne Laborausstattung für Hands-On Training und Übungen verwendet.

3 Einblick in eine Schulung im Lernlabor Cybersicherheit.

4 Lernkoffer des IOSB-INAs: Der Lernkoffer ist eine mobile Lernplattform und beinhaltet übliche Automatisierungskomponenten eines Schaltschranks der Produktionsanlage. Dadurch können Übungen zum Thema »IT-Sicherheit in der Automatisierungstechnik« direkt beim Kunden durchgeführt werden.

Mehr Sicherheit mit unseren Weiterbildungen

5 Gründe für die Weiterbildung im Lernlabor Cybersicherheit

5

Anerkannte Expertinnen und Experten

Profitieren Sie vom langjährigen Spezialwissen unserer Expertinnen und Experten aus der Forschung und unseren Entwicklungs- und Beratungsprojekten. In Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen erhalten Sie verwertbare, neueste Erkenntnisse auf allen Gebieten der Cybersicherheit.

Bei uns bekommen Sie Wissen aus erster Hand

Unsere Kurse sind nicht nur auf dem aktuellsten Stand der Forschung, sie orientieren sich auch passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Im Team trainieren und erarbeiten Sie Lösungskonzepte in den Bereichen, die für Sie tatsächlich relevant sind.

Maßgeschneiderte Inhouse-Seminare

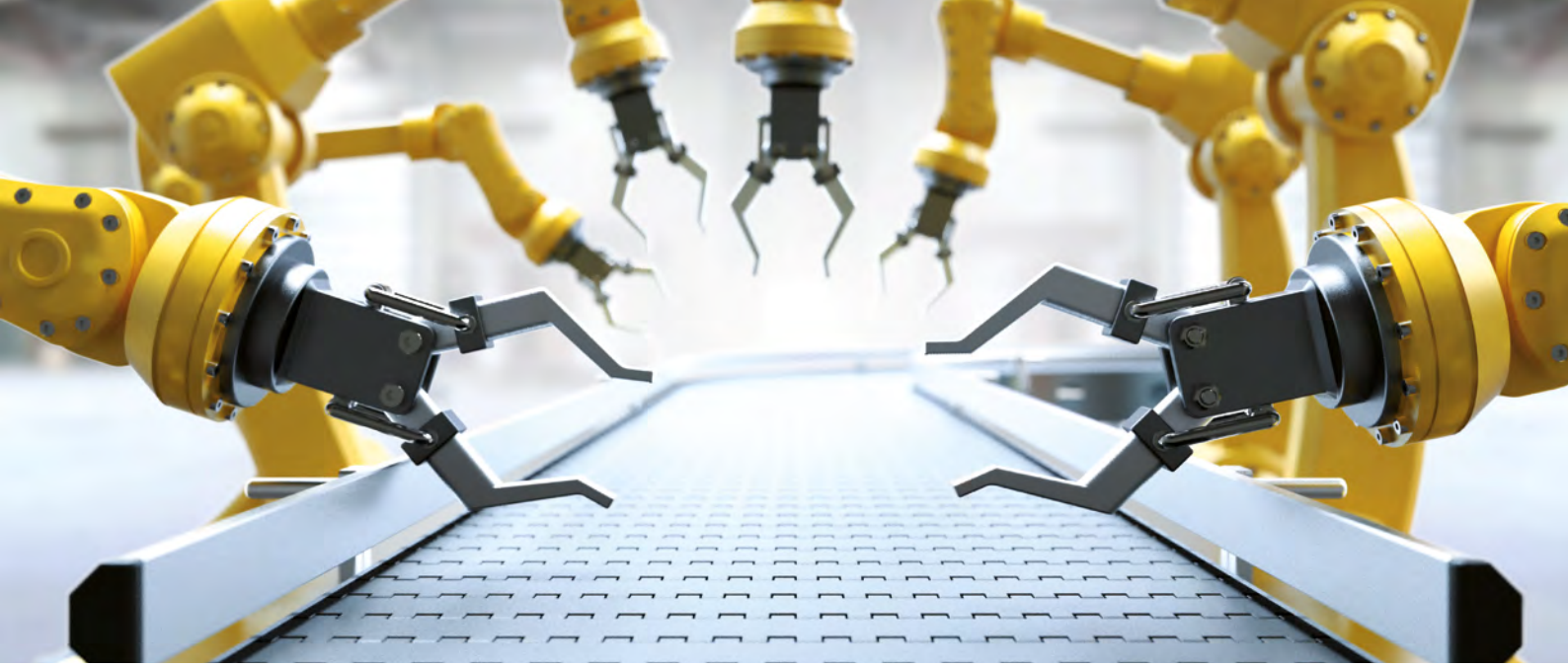
Integrieren Sie die Weiterbildung zum Thema Cybersicherheit direkt in Ihr Unternehmen, für mehrere Mitarbeitende oder Abteilungen. Dafür passen wir die Inhalte individuell auf Ihre Bedarfe an. Wir beraten Sie gerne, welche Lösung für Sie die optimale darstellt.

Für jede Situation das passende Seminar

Ein Universalkonzept bei IT-Sicherheitslösungen gibt es nicht! Die Komplexität und das Spektrum an Problemfeldern ist einfach zu groß. In unserem breiten Themenangebot finden Sie jedoch garantiert die passende Weiterbildung. Zugeschnitten auf Ihren Kenntnisstand und auf Ihr Spezialgebiet. Ob als Onlineseminar, Präsenzseminar oder Mix aus beidem.

Lernlabore

An zahlreichen Standorten in Deutschland können Sie in unseren modernen Lernlaboren mithilfe hochwertiger technischer Infrastruktur reale Bedrohungsszenarien nachstellen und durchspielen. Anhand konkreter Anwendungsfälle wird so das Gelernte für Sie erfahrbar und direkt umsetzbar.



Kompetenzaufbau auf allen Ebenen

IT-Sicherheitswissen betrifft nicht mehr nur Spezialistinnen und Spezialisten, auch entscheidungsbefugte Personen, Fachkräfte und Anwendende sollten lernen, Sicherheitsrisiken abzuschätzen und diese zu beherrschen. Hierfür benötigen die Mitarbeitenden eine Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und die Konsequenzen von IT-Sicherheitsproblemen in ihrem Verantwortungsbereich. Das Lernlabor richtet sich deshalb an folgende Zielgruppen mit jeweils spezifischen Seminaren:

Führungskräfte, die Entscheidungsprozesse verantworten müssen, benötigen einen verständlichen Überblick über aktuelle Gefahren, Sicherheitsstrategien und Methoden.

Sicherheitsexpertinnen und -experten mit einer IT-Sicherheits-ausbildung oder entsprechender Berufserfahrung können ihr Wissen auf den neuesten Stand bringen.

Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

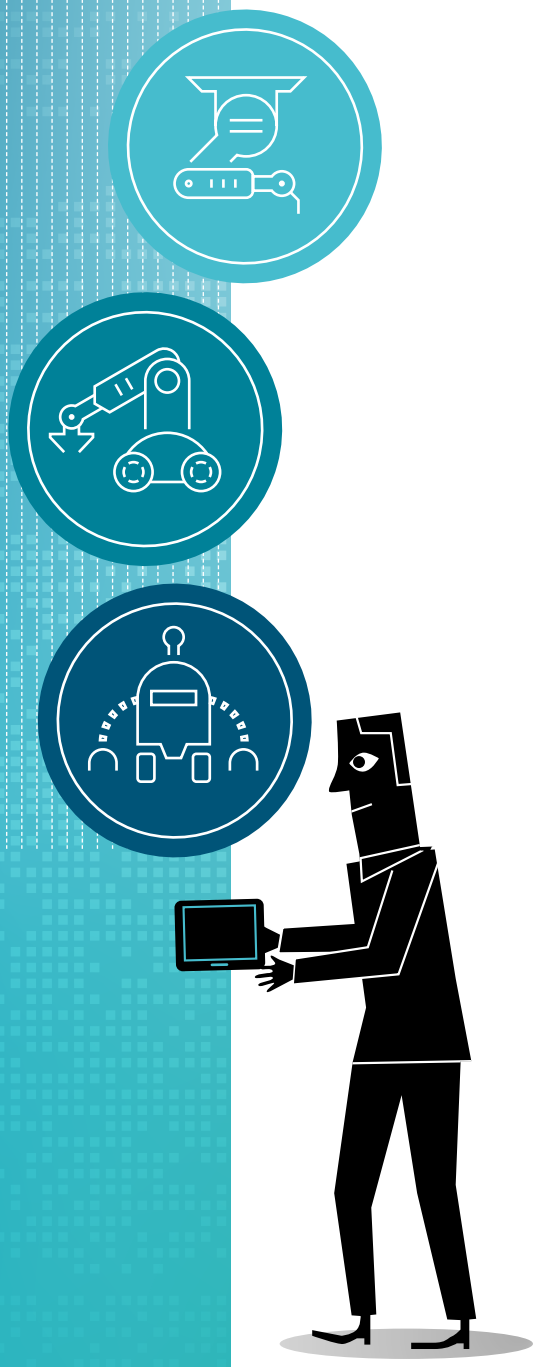
IT-Nutzerinnen und -Nutzer ohne spezifische Fachkenntnisse, von denen erwartet wird, dass sie Sicherheitsbewusstsein aufbauen und sicherheitskonformes Verhalten entwickeln.

Erklärung der Symbole auf den Seminarseiten

- Abschluss
- Voraussetzungen
- Zielgruppe
- Dauer
- Kosten
- Örtlichkeit

Industrielle Produktion

Anlagen vor Gefahren schützen!



Moderne Produktionsanlagen sind hochgradig vernetzt. Eingebettete Systeme kommunizieren selbstständig miteinander, Planungssysteme aus der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Anlagenführer überwachen und steuern aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus.

In der vernetzten Welt endet der Schutz von Produktionsanlagen nicht mehr am Gebäude oder am Fabrik-Gelände. Über die Netzwerk Verbindungen können Angreifer in die Systeme eindringen und diese manipulieren, Schadcode-Infektionen können weite Bereiche vollständig lahmlegen und dabei auch immense physische Schäden sowie Gefahren für Leib und Leben verursachen.

Unternehmen müssen im Zuge der digitalen Transformation ihre kritischen Systeme, Anlagen und Werte kennen, um geeignete Schutzmaßnahmen zu ergreifen. Dazu gehört, typische Schwachstellen in Design und Implementierung in eingebetteten Systemen und industriellen Komponenten zu kennen, zu identifizieren und zu vermeiden. Auch neueste Entwicklungen im Bereich von Kommunikationsprotokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software müssen in Automatisierungskomponenten und Produktionsanlagen umgesetzt werden, um sie effektiv schützen zu können.

Nicht erst seit Meldungen über Stuxnet, Duqu, Flame und Havex ist klar, dass Produktionsanlagen Ziele für Cyber-Angriffe sind.

Industrielle Produktion
Online

Industrial Demonstrator Attacks & Tools

Angriffe auf Industrieanlagen erleben

Die Herausforderung: Angriffe auf Industrieanlagen unterstreichen die Bedeutung der IT-Sicherheit für die industrielle Produktion. Was sind die häufigsten Bedrohungen? Was könnte tatsächlich passieren, wenn ein industrielles System angegriffen wird? Antworten auf diese Fragen finden Sie in unserem kurzen Online-Skill in Englisch.

Inhalte des Seminars

Einführung in einen speziell für Schulungen entwickelten Proof-of-Concept Demonstrator
- Eingesetzte Automatisierungskomponente,
- Kommunikationsverbindungen und Prozess

Erklärung und Demonstration von Angriffstechniken am Live-Demonstrator
- Reale Angriffstechniken in unterschiedlichen Angriffszenarien
- Nutzung typischer Angriffstools

Auswirkung von Angriffen live miterleben
- Auswirkungen der Angriffe auf den Prozess
- Potentielle Gegenmaßnahmen

Ihr Nutzen

- Awareness für die Gefährlichkeit von Cyberangriffen auf Produktionsanlagen.
- Erste Einführung in Angriffstechniken und mögliche Gegenmaßnahmen.

Informationen im Überblick

Grundlegende IT-Kenntnisse, grundlegende IT-Sicherheitskenntnisse von Vorteil

Komponentenhersteller*innen, Integratoren*innen, Maschinenbauer*innen, Betreibende von Automatisierungsanlagen, Dienstleistende

1 Std., 40 MInuten

100,–

online

Veranstaltet durch

University4Industry

Fraunhofer IOSB

Referenten:


Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB


M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB


Dipl.-Inform. Steffen Pfrang, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.university4industry.com/skills/industrial-demonstrator-attacks-tools

Industrielle Produktion
Präsenz | Online

Informationen im Überblick

Grundlegende IT-Sicherheitskenntnisse

Produktentwickelnde von Maschinenherstellern, Servicetechniker* innen bei Integratoren, Systemintegratoren*innen für Automatisierungskomponenten, Product Security Officer, Verantwortliche für Industrial Security

2 Tage

externe Veranstaltung, Preis wie bei Maschinenbau-Institut GmbH

Karlsruhe, Paderborn oder online

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IEM, Fraunhofer IOSB, University4Industry

Referenten:


Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB


M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB


M.Sc. Thorsten Koch, wiss. Mitarbeiter Fraunhofer IEM

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/security-by-design

Security by Design für Maschinen und Anlagen

IT-Sicherheit nach IEC 62443 von Beginn an mitdenken

Durch die Digitalisierung in der Industrie arbeiten Maschinen und Anlagen immer vernetzter und werden durch Embedded Software gesteuert. Dass die zunehmende Vernetzung nicht nur Vorteile bringt, ist spätestens seit Bekanntwerden diverser Sicherheitsvorfälle im Maschinenbau klar. Diese können Teile der Produktion oder im schlimmsten Fall die gesamte Fertigung lahmlegen. Deshalb müssen Hersteller von Maschinen und Anlagen bereits in der Entwicklungsphase die IT-Sicherheit mitdenken.

Inhalte des Seminars

Initialisierung
- Wichtige Begriffe, Schutzziele und Bedrohungen
- Grundlagen zu IEC 62443 und Security by Design

Analyse
- Bedrohungen und Risiken analysieren – eine Prozessbetrachtung
- Sicherheitsrisiken mit Security Assessments aufdecken

Entwurf
- Grundsätze für sichere System- und Softwarearchitekturen
- Sichere Vernetzung von Maschinen und Anlagen
- Sichere Komponenten – Anforderungen und ihre Beschaffung
- Risiken von Fernzugriffen einschätzen und Konzepte zur sicheren Umsetzung anwenden

Realisierung
- Grundsätze für die sichere Implementierung
- Prinzipien für manuelle und automatische Code-Reviews

Veröffentlichung
- Fail Securely und (In)Secure Defaults – Grundsätze für sicheres Deployment
- Systemhärtung – bewährte Vorgehensweisen und Fallstricke

Nutzung
- Aufgespürte Schwachstellen – Tipps für einen zielführenden Umgang
- Patch Management – Fehler beheben und Sicherheitslücken schließen

Ihr Nutzen

- Sie erfahren, wie Sie das Prinzip Secure by Design entlang Ihres Entwicklungsprozesses gewinnbringend einsetzen, um daraus möglichst sichere Maschinen und Anlagen für den Kunden zu produzieren.
- Sie lernen, relevante Sicherheitsrisiken frühzeitig zu erkennen, zu bewerten und geeignete Schutzmaßnahmen abzuleiten.

IT-Sicherheit in der Automatisierungstechnik

Vernetzen, aber sicher!

Die Herausforderung: Sichere Vernetzung in der Produktion. Mit zunehmender Vernetzung im Zuge der Industrie 4.0 steigt auch das Risiko für Cyberangriffe. Das Ausmaß solcher Angriffe kann von Nichtverfügbarkeit bis zum Totalausfall der Produktion reichen. In diesem Seminar werden bestimmte Angriffsmechanismen analysiert und Gegenmaßnahmen vermittelt. Darüber hinaus lernen Sie, wie bestehende Netzwerke analysiert und eine sichere Netzwerkinfrastruktur aufgebaut werden.

Ihr Nutzen

- In diesem Seminar lernen Sie die aktuellen Automatisierungssysteme kennen – vom klassischen System bis zum cyber-physischen Produktionssystem im Sinne der Industrie 4.0.
- Sie erhalten einen ganzheitlichen Ausblick auf das Thema Industrie 4.0 und seine sicherheitskritischen Aspekte – in praktischen Übungen und in der Theorie.
- Sie wenden etablierte Methoden zur sicheren Industrie 4.0-Kommunikation mit OPC UA an, um Industrie 4.0-Anwendungsfälle wie Condition Monitoring, Plug & Work und Optimierung zu realisieren.

Inhalte des Seminars

Industrie 4.0 & Automatisierungstechnik
- Digitalisierung und Vernetzung
- Sichere industrielle Kommunikation

Einführung in die Automatisierungstechnik
- Automatisierungssysteme
- Technische Prozesse
- Sensorik und Aktorik
- SPS-Programmierung

Netzwerkanalyse
- Aktive und passive Netzwerkanalyse
- Hard- & Software für die Netzwerkanalyse
- Angriffsszenarien

Grundlagen der Kryptographie
- Symmetrische vs. Asymmetrische Verschlüsselung
- Digitale Signaturen
- Kryptographische Hash-Funktionen
- Public Key Infrastructure (PKI)

Absicherung von Netzwerkinfrastruktur nach IEC 62443
- Grundlegende Anforderungen
- Zones & Conduits
- Security Levels
- OPC UA-Kommunikation

Informationen im Überblick

Grundlegende Kenntnisse in den Bereichen IT und Automatisierungstechnik sind von Vorteil, aber keine Voraussetzung

Entwickler*innen, Planende und Betreibende von Automatisierungstechnik; Personal aus der IT und/oder OT

3 Tage

1800,–

Lemgo oder online

Veranstaltet durch

Fraunhofer IOSB-INA

Referenten:

Dr.-Ing. Jens Otto, Gruppenleiter Fraunhofer IOSB-INA

M.Sc. Felix Specht, wiss. Mitarbeiter Fraunhofer IOSB-INA

M.Sc. Nils Koch, wiss. Mitarbeiter Fraunhofer IOSB-INA

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/it-sicherheit-automatisierungstechnik

Informationen im Überblick

Grundlegende Netzwerk- und IT-Kenntnisse von Vorteil, aber keine Voraussetzung

Komponentenhersteller, Personal aus dem Bereich Hardware- und Softwareentwicklung

3 Tage

1800,–

Lemgo oder online

Veranstaltet durch

Fraunhofer IOSB-INA

Referenten:

Dr.-Ing. Jens Otto, Gruppenleiter Fraunhofer IOSB-INA

M.Sc. Felix Specht, wiss. Mitarbeiter Fraunhofer IOSB-INA

M.Sc. Nils Koch, wiss. Mitarbeiter Fraunhofer IOSB-INA

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sichere-hardware-softwareplattformen

Sichere Hardware- und Softwareplattformen für Industrieprodukte

Von der Idee zum Produkt, aber sicher!

Die Herausforderung: Entwicklung sicherer Industrieprodukte. Um ein Industrieprodukt zu realisieren, müssen Anforderungen wie z. B. Sicherheit, Kosten, Portabilität und Support betrachtet werden. Dabei gibt es eine Vielzahl von unterschiedlichen Hardware- und Softwareplattformen sowie eine große Auswahl von Entwicklungsumgebungen und Programmiersprachen. Die Auswahl beeinflusst den Erfolg eines Industrieprodukts. Das Seminar gibt einen Einblick in die Entwicklung von Industrieprodukten.

Inhalte des Seminars

Sicherheitskonzepte im industriellen Umfeld
- Überblick IEC 62443
- Sicherer Produktlebenszyklus nach IEC 62443-4-1
- Sicherheitseigenschaften nach IEC 62443-4-2

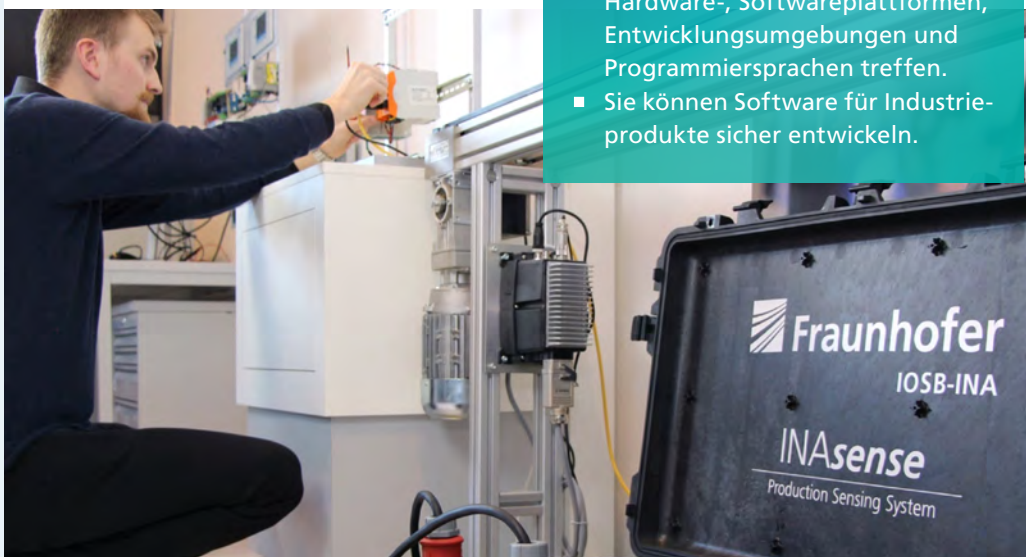
Hardwareplattformen und Betriebssysteme
- Eingebettete Betriebssysteme
- Auswahlprozess der Hardware

Absicherung von industriellen Endgeräten
- Systemhärtung
- Automatisierte Sicherheitsanalyse

Sichere industrielle Kommunikation
- OPC UA
- Verschlüsselte Verbindungen
- VPN
- WireGuard

Ihr Nutzen

- Das Seminar bietet Ihnen einen Einblick in die produktrelevanten Sicherheitskonzepte nach IEC 62443-4.
- Sie lernen aktuelle Betriebssysteme und Hardwareoptionen kennen.
- Nach diesem Seminar können Sie Anforderungen wie Sicherheit, Kosten, Portabilität und Support für ein Industrieprodukt bewerten.
- Sie können eine für Sie passende Auswahl aus unterschiedlichen Hardware-, Softwareplattformen, Entwicklungsumgebungen und Programmiersprachen treffen.
- Sie können Software für Industrieprodukte sicher entwickeln.



Industrielle Produktion
Präsenz | Online

Basiswissen IEC 62443

Absicherung cyber-physischer Systeme nach IEC 62443

Die Herausforderung: Entwicklung eines allumfassenden Cybersicherheitsmanagementsystems auf technischer und organisatorischer Ebene. Die Normreihe IEC 62443 bietet ein ganzheitliches Sicherheitskonzept mit dem Fokus auf Technologie, Prozesse und den Menschen. Teilnehmende erhalten einen Überblick über die verschiedenen Dokumente und Inhalte der Normreihe und lernen diese eigenständig anzuwenden. Dazu werden praktische Anwendungsbeispiele anhand von hochmoderner Laborinfrastruktur demonstriert.

Inhalte des Seminars

Einführung IEC 62443
- Übersicht und Zielgruppen
- Schutzziele IT vs. OT
- Unterschiede und Gemeinsamkeiten zu anderen Normen (ISO 2700er-Reihe)
- Begriffe und Definitionen

Cybersicherheitsmanagementsystem nach IEC 62443
- Überblick und Bestandteile eines CSMS
- Risikoanalyse
- Ausgewählte Gegenmaßnahmen
- Implementierung
- Monitoring und Optimierung des CSMS

Anforderungen an das System und Komponenten
- Bedrohungsanalyse
- Grundlegende Anforderungen
- Security Levels
- Protection Levels

Ihr Nutzen

- Sie bekommen eine detaillierte Einführung in den international Standard IEC 62443.
- Sie verstehen die Schutzziele und lernen die grundlegenden Anforderungen, um sie zu erreichen.
- Sie lernen Metriken wie Security Levels, mit denen sie die Sicherheit Ihres Produktionsnetzes bewerten können.
- Sie sind in der Lage, Konzepte wie Zones & Conduits umzusetzen und Risikoanalysen durchzuführen.
- Sie sind in der Lage, basierend auf Risiko- und Bedrohungsanalysen Gegenmaßnahmen zu entwickeln und sie umzusetzen.

Informationen im Überblick

Grundlegende Netzwerk- und IT-Kenntnisse von Vorteil, aber keine Voraussetzung

Komponentenhersteller, Integratoren, Anlagenbetreiber und (leitendes) Personal aus dem IT- und/oder OT-Umfeld

1 Tag

600,–

Lemgo oder online

Veranstaltet durch

Fraunhofer IOSB-INA

Referenten:

Dr.-Ing. Jens Otto, Gruppenleiter Fraunhofer IOSB-INA

M.Sc. Felix Specht, wiss. Mitarbeiter Fraunhofer IOSB-INA

M.Sc. Nils Koch, wiss. Mitarbeiter Fraunhofer IOSB-INA

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/basiswissen-iec-62443

Industrielle Produktion
Präsenz

Informationen im Überblick

Zertifikat

Einsteiger mit und ohne Vorwissen sowie Fortgeschrittene

Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion; Verantwortliche für die IT-Sicherheit; Entscheider*innen aus den genannten Bereichen

3 Tage

2475,–

Karlsruhe

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IOSB

Fraunhofer IOSB

Referenten:

Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB

M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-grundlagen

Cybersecurity nach IEC 62443 – Grundlagen

Einführung in die Industrial Security im Maschinenbau

Der IT-Sicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS) kommt im Maschinenbau eine besondere Bedeutung zu. Denn Cyberangriffe verursachen Produktionsausfälle, hohe Kosten und immense Imageschäden. Das Seminar zeigt Herstellern, Betreibern und Integratoren von vernetzten Maschinen und Anlagen auf, wie Industrial Security nach IEC 62443 für den Maschinenbau umgesetzt werden kann. Dabei wird die Theorie an zahlenreichen Beispielen und Demonstratoren veranschaulicht.

Die Maschinenbauer stehen vor der Herausforderung, dass Fachkräfte am Markt rar sind und sie deshalb das Know-how in Ihrem eigenen Unternehmen aufbauen müssen, um die IT-Sicherheit ihrer Produktion gewährleisten zu können.

Das Seminar (IC-32) führt in die wesentlichen Grundlagen zum Thema Industrial Security von Automatisierungs- und Steuerungsanlagen (IACS) im Maschinenbau ein. Dabei wird der Standard ISA/ IEC 62443 näher beleuchtet und ein umfassender Überblick über die Einsatzmöglichkeiten in der Produktion – auch an Hand von Fallbeispielen und Demonstratoren – gegeben.

Inhalte des Seminars

- Einführung in den IEC 62443 Standard
- Unterschiede zwischen IT- und OT-Security
- Einführung grundlegender Konzepte wie Defense-in-Depth, Zonen, Conduits und Security-Levels
- Aufbau eines Cyber Security Management Systems (CSMS)
- Einführung in die Themen Risikoanalyse und sicheres Systemdesign

Ihr Nutzen

- Sie lernen den Standard IEC 62443 und die zugrundeliegenden Konzepte kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.

Cybersecurity nach IEC 62443 – Risikobewertung

Die Risiken für Cyberangriffe auf IACS im Maschinenbau minimieren

Der erste Schritt in Richtung Industrial Security ist eine fundierte Bedrohungs- und Risikoanalyse (Thread Risk Assessment) der aktuellen Situation. Erst nach einer solchen Risikoabschätzung lassen sich geeignete Maßnahmen zur Absicherung der eingesetzten Automatisierungs- und Steuerungssysteme (industrial automation and control systems, IACS) im Maschinenbau ableiten. Das Seminar thematisiert die möglichen Risiken und zeigt, wie eine Risikoanalyse speziell für den Maschinenbau durchgeführt werden kann.

Die 4. Industrielle Revolution geht mit einer weitreichenden Automatisierung von industriellen Produktionsprozessen und somit der Vernetzung von industriellen Produktionssystemen einher. Ohne dies jedoch ausreichend abzusichern, sind Tür und Tor für Cyberangriffe und andere Bedrohungen geöffnet. Ein erster Schritt ist eine fundierte Risikobewertung der diversen Bedrohungen und Risiken, um darauf aufbauend Cybersecurity Requirements Specifications (CRS) abzuleiten. In diesem Seminar (IC-33) werden die Grundlagen vermittelt, um die Industrial Security von Automatisierungs- und Steuerungstechnik bewerten und Cybersecurity Requirement Specifications (CRS) ableiten zu können. Das Vorgehen bei einer Risikobewertung wird an Hand von praktischen Beispielen aus dem Maschinenbau und Demonstratoren gezeigt.

Inhalte des Seminars

- Vorgehen zur Schwachstellen-Identifikation
- Risikobewertung für ein IACS: Organisation und Durchführung
- Realistische Bedrohungsszenarien identifizieren und bewerten
- Lücken in bestehenden Richtlinien, Verfahren und Standards identifizieren
- Sicherheitszonen und -conduits einrichten und dokumentieren
- Dokumentation der Ergebnisse

Ihr Nutzen

- Sie lernen den Standard IEC 62443 mit Blick auf die Risikobewertung kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau und Demonstratoren.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.

Informationen im Überblick

Zertifikat

Einsteiger*innen mit geringem und ohne Vorwissen

Entscheider*innen, Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion, Verantwortliche für die IT-Sicherheit

3 Tage

2475,–

Karlsruhe

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IOSB

Fraunhofer IOSB

Referent:

Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB

M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-risikobewertung

Informationen im Überblick

Zertifikat

Einsteiger*innen mit geringem und ohne Vorwissen

Entscheider*innen, Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion, Verantwortliche für die IT-Sicherheit

3 Tage

2475,–

Karlsruhe

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IOSB

Fraunhofer IOSB

Referenten:

Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB

M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-it-sicherheitskonzept

Cybersecurity nach IEC 62443 – IT-Sicherheitskonzept

Sicherheitsanforderungen für vernetzte Maschinen und Anlagen definieren

Basierend auf einer fundierten Bedrohungs- und Risikoanalyse (Thread Risk Assessment) kann ein IT-Sicherheitskonzept für industrielle Automatisierungs- und Steuerungssystemen (IACS) entwickelt werden. Das Seminar zeigt speziell für Hersteller, Betreiber und Integratoren von Maschinen und Anlagen, wie eine solches Konzept mit entsprechenden Sicherheitsmaßnahmen und Testplänen erstellt werden kann.

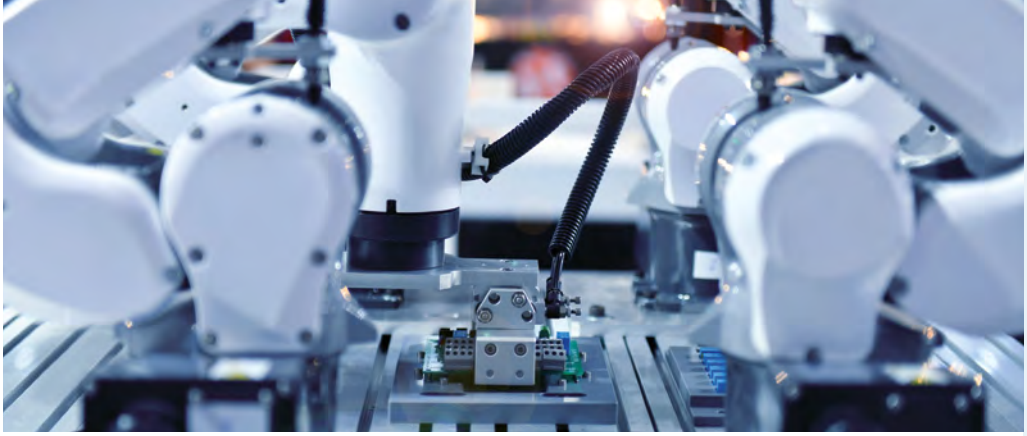
Die IT-Sicherheit von vernetzten Maschinen und Anlagen wird immer mehr zu einem Schlüsselthema für produzierende Unternehmen, vor allem aber für den Maschinenbau. Neben Produktionsausfällen fallen hohe Kosten an und entstehen immense Imageschäden. Um dies zu vermeiden, müssen Maschinenbauer mehr in die Cybersicherheit ihrer industriellen Produktionssysteme investieren. In diesem Seminar werden das notwendige Wissen und die Fähigkeiten vermittelt, um aufbauend auf einer Risikoanalyse Sicherheitsmaßnahmen für neue und bestehende IACS auswählen und umsetzen zu können. Darüber hinaus wird gezeigt, wie Testpläne zur Überprüfung von umgesetzten Maßnahmen in Verbindung mit den Sicherheitsanforderungen erstellt werden.

Inhalte des Seminars

- Ergebnisse einer Bedrohungs- und Risikoanalyse (Thread Risk Assessment) interpretieren
- Entwicklung einer Cybersecurity Requirements Specification (CRS) und darauf basierenden Konzepten
- Den Security Development Lifecycle und dessen Bestandteile verstehen
- Durchführung einer grundlegenden Konfiguration und Inbetriebnahme einer Firewall
- Eine sichere Lösung für den Remote-Zugang entwickeln
- Entwicklung einer Spezifikation zur Systemhärtung
- Umsetzung eines einfachen Intrusion Detection Systems (IDS)
- Entwicklung und Durchführung eines Cybersecurity Acceptance Test Plan (CFAT/CSAT)

Ihr Nutzen

- Sie lernen den Standard IEC 62443 mit Blick auf die Entwicklung eines IT-Sicherheitskonzepts kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau und Demonstratoren.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.



Cybersecurity nach IEC 62443 – Sicherer Betrieb und Instandhaltung

Die IT-Sicherheit über den gesamten Produktlebenszyklus sicherstellen

Industrial Security ist keine einmalige Sache, sondern muss nach dem Legen der Grundlagen kontinuierlich sichergestellt werden. Dazu gehört es, das IT-Sicherheitskonzept umzusetzen und weiterzuentwickeln, aber auch die etablierten Maßnahmen zu kontrollieren. Das dafür notwendige Know-how wird in diesem Seminar speziell für den Maschinenbau an Hand von Beispielen und Demonstratoren vermittelt. Cyberangriffe und andere Bedrohungen auf industrielle Automatisierungs- und Steuerungsanlagen (IACS) abzuwenden, ist mittlerweile ein Muss. Dabei reicht es nicht nur, ein IT-Sicherheitskonzept zu erstellen. Es muss konsequent weiterentwickelt und verbessert werden, so dass die entsprechenden Sicherheitsmaßnahmen effektiv greifen können.

Ziel des Seminars (IC-37) ist es, den sicheren Betrieb von industriellen Produktionssystemen über den kompletten Lebenszyklus bis hin zur Außerbetriebnahme sicherzustellen.

Inhalte des Seminars

- Einfache Netzwerkdiagnosen durchführen
- Diagnose- und Ereignismeldungen richtig interpretieren
- Backup- und Wiederherstellungskonzepts umsetzen
- Change Management System etablieren
- Patch Management Cycle beschreiben
- Einsatz von Antivirus-Systemen und einfacher Werkzeuge zur Applikationsüberwachung
- Einfache Netzwerk- und Host-Intrusion-Detektionssystemen einsetzen
- Einsatz einfacher Sicherheitsvorfall- und Ereignisüberwachungstools
- Einen Incident Response Plan umsetzen

Ihr Nutzen

- Sie lernen den Standard IEC 62443 mit Blick auf die Sicherstellung von IACS während des gesamten Betriebs kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau und Demonstratoren.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.

Industrielle Produktion
Präsenz

Informationen im Überblick

Zertifikat

Einsteiger*innen mit geringem und ohne Vorwissen

Entscheider*innen, Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion, Verantwortliche für die IT-Sicherheit

3 Tage

2475,–

Karlsruhe

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IOSB

Fraunhofer IOSB

Referent:

Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB

M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-betrieb-instandhaltung

Informationen im Überblick

Fachkräfte mit ausreichendem Vorwissen

Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion, Verantwortliche für die IT-Sicherheit die die Industrial Security in ihrem Unternehmen sicherstellen sollen.

5 Tage

6250,–

Präsenz

Veranstaltet durch
Maschinenbau-Institut GmbH in Kooperation mit Fraunhofer IOSB

Fraunhofer IOSB

Referenten:

Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB

M.Sc. David Meier, wiss. Mitarbeiter Fraunhofer IOSB

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-fortgeschrittene

Cybersecurity nach IEC 62443 – Kompaktkurs Fortgeschrittene

Expert*in für die IT-Sicherheit von industriellen Produktionssystemen werden

Industrielle Produktionssysteme und klassische Informationssysteme haben eines gemeinsam: sie sind beide gleichermaßen Cyberangriffen und anderen Bedrohungen aus dem Netz ausgesetzt. Davon ist besonders der Maschinenbau als Teil des produzierenden Gewerbes betroffen. Dementsprechend wichtig ist es, Industrial Security zu etablieren, d.h. die eingesetzten Automatisierungs- und Steuerungssysteme (IACS) zu schützen.

Hersteller, Integratoren, Dienstleister und Betreiber müssen gleichermaßen dafür sorgen, dass ihre industriellen Automatisierungs- und Steuerungssysteme (industrial automation and control systems, IACS) über den gesamten Produktlebenszyklus hinweg gegen Cyberangriffe und andere Bedrohungen abgesichert sind. Die internationale Normenreihe IEC 62443 beinhaltet für alle Beteiligten in den unterschiedlichen Phasen des Lebenszyklus Hilfestellungen für die Entwicklung und Umsetzung der Industrial Security.

Der Kompaktkurs behandelt alle Maßnahmen zur Sicherstellung der Industrial Security speziell für den Maschinenbau. Von der Risikoanalyse und -bewertung bis zur Erstellung eines IT-Sicherheitskonzepts bis hin zur Umsetzung im laufenden Betrieb werden alle Phasen mit Fallbeispielen aus der Praxis veranschaulicht.

Ihr Nutzen

- Sie lernen den Standard IEC 62443 und die zugrundeliegenden Konzepte kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau und Demonstratoren.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.

Inhalte des Seminars

Bedrohungslage für industriellen Automatisierungs- und Steuerungsanlagen (IACS)

Einführung in die Normenreihe IEC 62443

Bedrohungs- und Risikoanalyse nach IEC 62443 in der Praxis

IT-Sicherheitskonzept entwickeln

Maßnahmen zum sicheren Betrieb und Instandhaltung entwickeln und umsetzen

Industrielle Produktion
Online

Informationen im Überblick

Keine Voraussetzungen

Fachkräfte, Entwickler*innen und Spezialist*innen für Industriekomponenten

2 Tage jeweils von 09:00 bis 12.30 Uhr

799,–

online

Veranstaltet durch
secuvera GmbH in Kooperation mit dem Fraunhofer IOSB-INA

Fraunhofer IOSB-INA

Industrial SDL Workshop

Sicherer Entwicklungsprozess für Industriekomponenten nach IEC 62443

Bei der Realisierung von Industriekomponenten müssen verschiedenen Anforderungen betrachtet werden und ein sicherer Entwicklungsprozess (SDL, Security Development Lifecycle) eingehalten werden. Eine Zertifizierung nach IEC 62443 erlaubt den Nachweis, eine Industriekomponente sicher entwickeln zu können.

Inhalte des Seminars

Überblick sicherer Entwicklungsprozess

Sicherheitsrelevante Anforderungen, Entwurf und Implementierung entlang einer Beispielkomponente

Verifikation & Testen einer Industriekomponente mit Beispielen zu Test-Werkzeugen

Veröffentlichung und Reaktion auf Fehler und Schwachstellen

Ihr Nutzen

- Sie erhalten tiefe Einblicke in einen sicheren Entwicklungsprozess für Industriekomponenten nach der IEC 62443 und den dort beschriebenen SDL-Prinzipien.
- Nach dem Seminar haben Sie einen Überblick über die notwendigen Schritte und können diese schrittweise in Ihre Entwicklung integrieren.
- Im Austausch mit Fachexperten und anhand praxisnaher Übungen können Sie die Inhalte vertiefen.

Referenten:


Sebastian Fritsch, Leiter des Bereichs BSI-Prüfstelle & Industrial Security


Ruben Konrad, Prüfer für IEC 62443 und Common Criteria


Dr.-Ing. Christian Haas, Gruppenleiter Fraunhofer IOSB


Dr.-Ing. Jens Otto, Gruppenleiter Fraunhofer IOSB-INA

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/industrial-sdl

Inhouse- oder Firmen- und Behördenschulungen

Inhouse-Schulungen individuell auf Sie zugeschnitten

Wollen Sie Inhalte aus unserem Kursangebot individuell zusammenstellen, oder finden Sie in unserem Angebot keinen passenden Termin oder Ort? Kein Problem: Stellen Sie Ihre ganz persönlichen Bedürfnisse in den Vordergrund.

Sie haben die Wahl, so geht's:

- Wählen Sie ein Wunschseminar aus unseren vielfältigen Themen aus und bestimmen Sie den Zeitraum und Schulungsort.
- Nennen Sie uns Inhalte aus unseren Kursangeboten, die geschult werden sollen, und wir konzipieren ein passendes Seminar.
- Sie sagen uns, welches spezielle Wissen geschult werden soll, und wir entwickeln eine individuelle Schulung für Sie.

Bei einem individuellen Inhouse-Seminar erhalten Sie genau auf Ihre Bedürfnisse abgestimmtes Wissen – für Ihr Unternehmen, Abteilungen Ihres Unternehmens, für Ihre Behörde, Fachreferate oder einzelne Mitarbeiterinnen und Mitarbeiter. Dabei stehen wir Ihnen sehr gerne beratend zur Verfügung, wenn es um für Sie maßgeschneiderte, inhaltliche Zusammenstellung der vielfältigen Kombinationsmöglichkeiten unserer Themen geht.

Wir als Lernlabor Cybersicherheit bieten Ihnen alle relevanten Elemente aus einer Hand: Die didaktische, mediale sowie technische Umsetzung der Inhalte, aber auch Konzept und Umsetzung.

Fragen Sie uns an!

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne

telefonisch unter +49 89 1205-1555

e-mail: cybersicherheit@fraunhofer.de

www.cybersicherheit.fraunhofer.de

Hier erhalten Sie aktuelles Wissen!

Aktuelle Informationen zu unseren Seminarangeboten, Veranstaltungen und Themen im Bereich Cybersicherheit finden Sie hier:

www.cybersicherheit.fraunhofer.de

Stöbern Sie in unserem Blog und erfahren Sie, was unsere Fachexpertinnen und -experten über aktuelle Themen im Bereich Cybersicherheit berichten:

www.cybersicherheit.fraunhofer.de/de/blog

Abonnieren Sie unseren Newsletter und bleiben Sie so auf dem Laufenden:

www.cybersicherheit.fraunhofer.de/newsletter

Weitere Informationen rund um das Thema Weiterbildung bei der Fraunhofer Academy erhalten Sie hier:

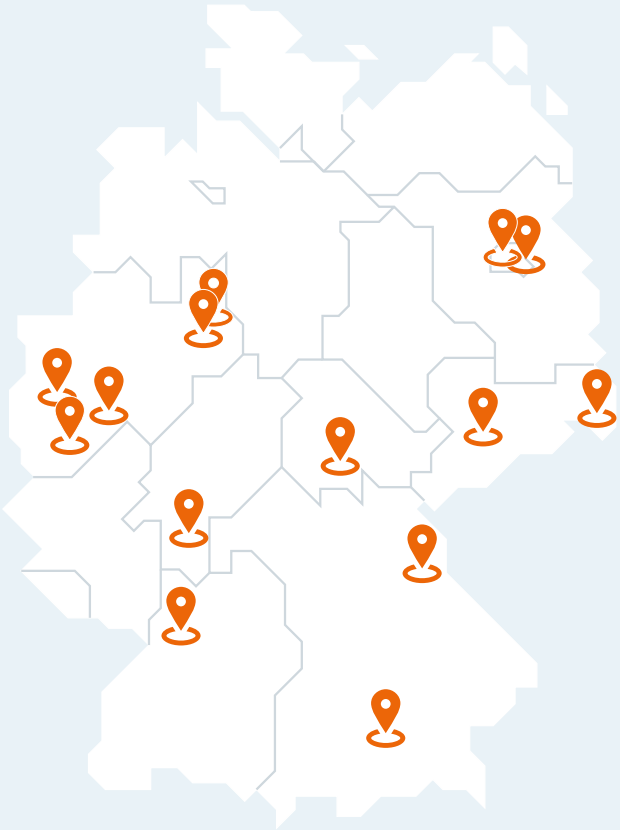
Aktuelle Qualifizierung aus der angewandten Forschung

Das Lernlabor Cybersicherheit ist ein Weiterbildungsprogramm, in dem Expertinnen und Experten von Fraunhofer und ausgewählten Fachhochschulen aktuellste Erkenntnisse auf dem Gebiet der Cybersicherheit vermitteln. Die Lehrmodule werden von den beteiligten Fraunhofer-Instituten und Fachhochschulen entwickelt und weitergegeben. Die Fraunhofer Academy ist die Geschäftsstelle und Plattform der Initiative, die Entwicklung, Vermarktung, Teilnehmermanagement und Qualitätssicherung koordiniert. Das Programm wird durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Die beteiligten Partnerhochschulen

- Ostbayerische Technische Hochschule Amberg-Weiden
- Hochschule für Technik und Wirtschaft Berlin
- Hochschule Bonn-Rhein-Sieg
- Hochschule Mittweida
- Hochschule Niederrhein
- Technische Hochschule Ostwestfalen-Lippe
- Hochschule Zittau/Görlitz

Standorte der Lern- und Forschungslabore der beteiligten Fraunhofer-Institute und Fachhochschulen



Die beteiligten Fraunhofer-Institute

- Fraunhofer AISEC
- Fraunhofer FKIE
- Fraunhofer FOKUS
- Fraunhofer IEM
- Fraunhofer IOSB
- Fraunhofer IOSB-AST
- Fraunhofer IOSB-INA
- Fraunhofer SIT

Know-how schafft Sicherheit! Seit 5 Jahren unterstützen wir deshalb Unternehmen auf dem Weg zu mehr IT-Sicherheit.«

Dr. Raphaela Schätz,
Qualitäts- und Programm Management
im Lernlabor Cybersicherheit

Herausgeber

Fraunhofer Academy
Hansastraße 27c
80686 München

Telefon +49 89 1205-1555
Fax +49 89 1205-77-1599

cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Redaktion: Elly Leimenstoll

Layout und Satz, Illustrationen:
Vierthaler & Braun

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne
- telefonisch unter + 49 89 1205-1555
- per E-Mail: cybersicherheit@fraunhofer.de
- auf unserer Website unter

www.cybersicherheit.fraunhofer.de

Wir beraten Sie gerne, welche Weiterbildungen und Inhalte für Sie hilfreich sind.

Sie suchen nach Angeboten für Ihr Team?

Für Unternehmen bieten wir Inhouse-Schulungen und unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung. Wir erheben gemeinsam mit Ihnen den Kompetenzbedarf in Ihrer Abteilung oder Firma und beraten Sie, die richtigen Fähigkeiten in Ihrer Organisation aufzubauen.

Adem Salgin

Ihr Ansprechpartner im Lernlabor Cybersicherheit

Seminarberatung
und Anmeldung

Möchten Sie Informationen zu einem anderen Themengebiet?

Hier finden Sie alle Broschüren rund um die Weiterbildungen im Lernlabor Cybersicherheit: www.cybersicherheit.fraunhofer.de/downloads

Stand Mai 2022

Sie erreichen uns

– telefonisch unter +49 89 1205-1555
– per E-Mail: cybersicherheit@fraunhofer.de
– auf unserer Website unter

www.cybersicherheit.fraunhofer.de