Fraunhofer ACADEMY

Weiterbildung für Cyber-Resilienz

Digitale Stärke neu gedacht

In einer Welt, in der digitale Bedrohungen ständig zunehmen, ist Cyber-Resilienz der Schlüssel zum Fortbestand und Erfolg von Unternehmen. Unser Angebot geht weit über die bloße Einhaltung von Gesetzen hinaus und zielt darauf ab, Unternehmen umfassend für die Herausforderungen der Cybersicherheit zu rüsten.
Durch unsere anwendungsorientierte Forschung mit unterschiedlichen Unternehmen/Partnern verstehen wir, dass jedes Unternehmen und jede Branche einzigartige Anforderungen hat. Daher berücksichtigen wir neben der Compliance vor allem Industrie-Best-Practices und unternehmensspezifische Bedürfnisse, um den Cyber-Resilienz-Status Ihres Unternehmens ganzheitlich zu erfassen und zu verbessern.

Wir machen Sie fit für die Cyber-Resilienz. Dies erreichen wir durch:

- Maßgeschneiderte Schulungen, die auf Ihr Unternehmen, Ihre Branche und die geltenden Informationssicherheitsvorgaben zugeschnitten sind
- Einen ganzheitlichen Ansatz, der über das gesetzliche Minimum hinausgeht
- Praxisnahe Vorbereitung auf potenzielle Cyberangriffe

Mit unserem Weiterbildungsangebot sind Sie bestens gerüstet, um den wachsenden Herausforderungen der Cybersicherheit proaktiv zu begegnen und die Widerstandsfähigkeit Ihres Unternehmens nachhaltig zu stärken.

So entwickeln wir Ihre individuelle Inhouse-Schulung

1 Analyse

Gemeinsam klären wir Ihre **Anforderungen** in einem Assessment oder Quick-Check

2 Beratung & Konzeption

Wir entwickeln ein individuelles und **bedarfsgerechtes** Schulungs-Konzept

3 Durchführung & Evaluation

Wir setzen die Schulungen um und werten mit Ihnen den **Anwendungserfolg** aus

Unser Schulungs-Angebot zu Cyber-Resilienz:

Grundlagen des Cyber Resilience Act (CRA): Pflichten kennen und proaktiv handeln
Web Based Training
Einführung zu den rechtlichen Aspekten des CRA mit theoretischem Wissen und konkreten Handlungsempfehlungen zur Vorbereitung auf die CRA-Einhaltung und Verbesserung der Cyber-Resilienz von Produkten.

- Auswirkungen des CRA auf Unternehmen
- Implementierung der CRA-Anforderungen
- Strategien zur Verbesserung der Produkt-Cyber-Resilienz

Cyber-Resilienz-Training für Softwarearchitekten
Inhouse-Format
Effektive Schutzstrategien für moderne Softwarearchitekturen gegen Cyberbedrohungen.

- Präventive und reaktive Maßnahmen zur Resilienzsteigerung
- Schlüsselkonzepte für resiliente Architekturen
- DevSecOps und Cloud-Resilienz

Software Security Training für Product Owner & Führungskräfte
Inhouse-Format
Verständnis für Cyber-Resilienz vertiefen und praktische Implementierungsstrategien erwerben.

- Cyber-Resilienz-Grundlagen für zukunftsorientierte Unternehmen
- Risikomanagement der Produktentwicklung
- Integration von Resilienz in den Produktlebenszyklus
- Förderung einer Sicherheitskultur

Business Continuity Management (BCM)
Präsenz-Seminar oder Inhouse-Format
Praxisorientierte Schulung für effektive BCM-Implementierung, Kernwissen zur Geschäftskontinuität in Krisen.

- BCM-Grundlagen und -Relevanz
- Strategieentwicklung und Schlüsselprozess-Identifikation
- Notfallplanung und unternehmensweite Integration

Cyber-Resilienz für die Energie- und Wasserversorgung
Präsenz-Seminar oder Inhouse-Format
Absicherung der kritischen Infrastruktur anhand der fünf Phasen der Cyber-Resilienz. Analyse der IT-Infrastruktur anhand praxisnaher Übungen und realer Fallbeispiele.

- Risikobewertung in Versorgungssystemen
- Implementierung von Schutzmaßnahmen
- Integration von Cyber-Resilienz in bestehende Infrastrukturen
- Werkzeuge und Maßnahmen für die fünf Phasen der Cyber-Resilienz

Cyber-Resilienz-Training für Produktentwickler von eingebetteten Systemen
Inhouse-Format
Verbindung von theoretischen Grundlagen mit praxisnahen Übungen, um Cyber-Resilienz-Strategien effektiv in Embedded-Projekte zu integrieren.

- Risiken in der Embedded-Entwicklung erkennen
- Sicherheit in ressourcenknappen Umgebungen
- Cyberresiliente Embedded-Systeme: Best Practices
- Sicherheit im Produktlebenszyklus integrieren

Hacking und Härtung von Machine Learning-Modellen
Präsenz- und Online-Seminar
Cyber-Resilienz im Kontext von KI und Machine Learning, mit theoretischem Wissen und praktischen Übungen.

- Identifikation von ML-Modell-Schwachstellen bzgl. Sicherheit und Privacy
- Angriffe auf Deeplearning-Classifiers und Large Language Models (LLM); Deepfake-Angriffe
- Entwicklung von Schutzmaßnahmen für ML-Modelle
- Implementierung sicherer ML-Pipelines für verschiedene Modalitäten

Fragen oder Wünsche?

Für Ihr Unternehmen ist noch nicht das Passende dabei? Oder Sie möchten Ihre Anforderungen vorab in einem Assessment überprüfen lassen? Nehmen Sie mit uns Kontakt auf für ein individuelles Angebot!

Lernlabor Cybersicherheit
E-Mail: cybersicherheit@fraunhofer.de
Telefon: +49 89 1205 1555

www.cybersicherheit.fraunhofer.de