

MODULÜBERSICHT

SECURITY ENGINEERING

- **EINFÜHRUNGSVERANSTALTUNG**
Veranstaltungsauftakt, Programminstallation und Lernvorbereitung
- **CYBER SECURITY**
Dozent: Prof. Dr. Thomas Smits
- **SOFTWARE SECURITY**
Dozent: Prof. Dr. Sachar Paulus
- **PRODUCT SECURITY**
Dozent: Prof. Dr. Thomas Smits, Prof. Dr. Sachar Paulus

Veranstaltungsauftakt, Programminstallation und Lernvorbereitung

EINFÜHRUNGSVERANSTALTUNG

LERNZIELE

Nach der Einführung können die Teilnehmenden...

- den Ablauf und die Ziele der Weiterbildung verstehen.
- die benötigten Programme und Tools installieren und starten.
- die Lernplattform und bereitgestellten Materialien nutzen.
- sich auf die Weiterbildung vorbereiten (Organisation, Zeitplanung, technische Voraussetzungen).
- die zuständigen Ansprechpersonen für technische und organisatorische Fragen benennen.

MODULÜBERSICHT SECURITY ENGINEERING

Dozent: Prof. Dr. Thomas Smits

CYBER SECURITY



LERNFORM

Präsenz + Live-Online



ORT

Hochschule Aalen



DAUER

5 (Online-)Präsenztage,
E-Learning, Prüfungseinheit



ABSCHLUSS

Hochschulzertifikat mit ECTS nach bestandener
Prüfung, Teilnahmebescheinigung

LERNZIELE

Die Teilnehmenden sind in der Lage, Grundlagen sowie aktuelle Trends im Bereich der Cyber Security unter Verwendung von Methoden der Künstlichen Intelligenz zu diskutieren, zu analysieren und Lösungskonzepte zu erarbeiten.

- Sichtweisen auf die Cyber Security
- Sicherheitsmanagement
- Kryptographie
- Sicherheit im Internet
- Public Key Infrastructure (PKI)
- Identifikation und Authentifikation
- Netzwerksicherheit
- Künstliche Intelligenz und Cyber-Sicherheit



MODULÜBERSICHT SECURITY ENGINEERING

Dozent: Prof. Dr. Sachar Paulus

SOFTWARE SECURITY



LERNFORM

Präsenz + Live-Online



ORT

Hochschule Aalen



DAUER

5 (Online-)Präsenztage
inkl. Prüfungsleistung +
E-Learning



ABSCHLUSS

Hochschulzertifikat mit ECTS nach bestandener
Prüfung, Teilnahmebescheinigung

LERNZIELE

Die Teilnehmenden sind in der Lage, die „Industry Best Practices“ im Bereich der sicheren Software-Entwicklung auf Software im Umfeld des Autonomen Fahrens anzuwenden. Dies umfasst sowohl analytische („Penetration Testing“) als auch konstruktive („Secure SDL“) Vorgehensweisen.

- Grundsätze der sicheren Software-Entwicklung, Vorgehensmodelle und Prozesse, einschlägige Normen und Standards
- Sicherheitsanforderungen
- Sicheres Design und Bedrohungsmodellierung, Architekturanalysen, Security Design Patterns
- Sicherheitstests, Penetrationstests, Tools zum Testen
- Sichere Einrichtung und sicherer Betrieb
- Security Response: Umgang mit Schwachstellen, die durch andere entdeckt werden



MODULÜBERSICHT SECURITY ENGINEERING

Dozent: Prof. Dr. Thomas Smits, Prof. Dr. Sachar Paulus

PRODUCT SECURITY



LERNFORM

Präsenz + Live-Online



ORT

Hochschule Aalen



DAUER

5 (Online-)Präsenztage
inkl. Prüfungseinheit



ABSCHLUSS

Hochschulzertifikat mit ECTS nach bestandener
Prüfung, Teilnahmebescheinigung

LERNZIELE

Die Teilnehmenden lernen Sicherheitsanforderungen für digitale Produkte zu analysieren und setzen geeignete technische sowie organisatorische Maßnahmen um. Sie erkennen typische Schwachstellen in Netzwerken, Webanwendungen und Betriebssystemen, integrieren Security in Entwicklungsprozesse und härten Systeme zielgerichtet. Zudem verstehen sie relevante Standards und Managementsysteme und können Sicherheitsprozesse strukturiert im Produktkontext anwenden.

Netzwerksicherheit

- Grundlagen von Netzwerken und TCP/IP verstehen
- Sichere Kommunikation und Verschlüsselung umsetzen
- Firewalls, Netzwerksegmentierung und Intrusion Detection anwenden

Web Security

- Typische Schwachstellen und Angriffe auf Webanwendungen erkennen
- Penetration Testing praxisnah durchführen (z. B. mit Burp Suite/DVWA)

Sichere Softwareentwicklung

- Prinzipien sicherer Softwareentwicklung in simulierten Pipelines anwenden
- Sicherheitsmaßnahmen systematisch in Entwicklungsprozesse integrieren

Betriebssystemsisicherheit

- OS-Grundlagen und Security-Konzepte verstehen
- Betriebssysteme und Embedded Systems härten und absichern
- Secure Boot und OTA-Updates berücksichtigen

Management-Systeme für IT-Sicherheit

- Relevante Standards und Managementsysteme (ISMS, CSMS, ISO 62443, ISO/SAE 21434) kennen
- Sicherheitsprozesse strukturiert in Organisationen implementieren

