Seminarort

CCG-Zentrum, Technologiepark
Argelsrieder Feld 22, Geb. TE 03, D-82234 Weßling-Oberpfaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

Gebühr

EUR 1.490,--
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Umsatzsteuer befreit. Für Veranstaltungen an ausländischen Standorten gelten die dortigen Steuerregelungen.

Mitglieder der CCG erhalten 10% Rabatt. Studentenrabatte sind auf Nachfrage verfügbar. Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte melden Sie sich möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 22, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12
E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

Rudolf Huber
MBDA GmbH Deutschland GmbH, Schrobenhausen
rudolf.huber@mbda-systems.de

Stornierung

Bei Stornierungen, die später als 14 Tage vor Seminarbeginn eingehen, werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist selbstverständlich möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus anderen triftigen Gründen ein Seminar bis 14 Tage vor Beginn abzusagen. Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

Cyber Security

Carl-Cranz-Gesellschaft e.V. | Weßling

Gesellschaft für technisch-wissenschaftliche Weiterbildung

Seminar IN 6.47

Informationssicherheit / Cyber Security in der Produktentwicklung im militärischen Bereich

17. - 18. September 2025
Oberpfaffenhofen bei München

Informatik

Wissenschaftliche Leitung

Rudolf Huber
MBDA Deutschland GmbH, Schrobenhausen
Jochen Veith
Diehl Defence GmbH & Co. KG, Röthenbach a. d. Pegnitz

Seminarprogramm

Mittwoch, 17.09.2025
08:30 – 16:30 Uhr

08:30 – 08:45	**Begrüßung, Organisation**
08:45 – 10:15 R. Huber	**Terminologie, Situation und Grundlagen** Warum Cybersecurity: Bedeutung, Bedrohungslage, grundsätzliche Einordnung • Grundlagen der Informationssicherheit, Schutzziele, Terminologie, Grundsätzliche Maßnahmen • Besonderheiten militärischer Systeme • Abgrenzung zu einer Firmeninfrastruktur
10:30 – 11:30 R. Huber	**IT Security in Product, Supply Chain und Test/Development Tools** Beschreibung der 3 Bereiche, Darstellung möglicher Bedrohungen im jeweiligen Bereich • Skizzenhafte Beschreibung möglicher Verfahren / Vorgehen in den Bereichen
12:30 – 13:30 J. Veith R. Berndt	**Typische Dokumentenlandschaft und Prozesse auf dem Weg zur Akkreditierung und GeNu** Welche Dokumente gibt es, wer erstellt sie zu welchem Zeitpunkt • Beschreibung des Projektbezogenen Informationssicherheitskonzepts gem. ZDv A-960/1
13:45 – 14:45 15:00 – 16:30 T. Slany	**Überblick über amtliche Vorgaben IT-Grundschutz und relevante Standards sowie zugehörige Methodiken** Wichtige Normen und Standards (national, militärisch), kurze Beschreibung relevanter Normen • Einführung in die BSI IT-Grundschutz Methodik

Cyber Security

Donnerstag, 18.09.2025
08:30 – 17:30 Uhr

08:30 – 10:30 J. Veith R. Berndt	**IT-Grundschutz-Modellierung** Kurze Vorstellung eines Modellierungstools (am Beispiel SAVe) • Teamarbeit: Exemplarische Modellierung eines kleinen IT-Verbunds (nicht toolgestützt)
10:45 – 11:15 J. Veith R. Berndt	**Nationale Amtsstellen (DEUmilSAA, WTD81 zu Vermessung Abstrahlsicherheit)** Wer sind die zuständigen Amtsstellen, was ist deren jeweilige Aufgabe • Beschreibung der jeweiligen Schnittstellen
11:15 – 12:15 T. Slany	**Internationale Entsprechungen zum IT-Grundschutz im Hinblick auf internationale Projekte** Militärische Internationale Standards, NATO / EU • kurze Einführung in die Common Criteria; NIST
13:15 – 14:15 R. Huber	**Schutzüberlegungen jenseits IT-Grundschutz** Unterschied kommerzieller und militärischer Schutzbedarf • Interne Angreifer • Gegnerische Cyber-Operationen und Advanced Persistent Threats • Aktive Verteidigung • Resilienz nach teilweiser Zerstörung
14:30 – 15:30 R. Huber	**Robuste Konzepte und Mechanismen zur Verteidigung** Zero Trust • Blockchains
15:45 – 17:15 R. Huber	**Technische Ansätze für HW und SW Sicherheit, Entwicklungs- und Testumgebungen sowie Verfahren** Sichere Betriebssysteme • TPM und Tampering • Rust • Cyber-Labs
17:15 – 17:30	**Abschlussdiskussion**

Cyber Security

Teilnehmer

Das Seminar richtet sich an Projektleiter, Entwickler oder andere Interessierte, die sich einen Überblick (im Sinne eines Quick Start) über die verschiedenen Aspekte und Standards der IT-Security in der Produktentwicklung und im Produkt verschaffen wollen. Ziel des Seminars ist die Teilnehmer zu befähigen mit den entsprechenden IT-Security-Spezialisten zielgerichteter und produktiver zusammen zu arbeiten, um Produkte erfolgreich zur Akkreditierung und GeNu zu führen.

Seminarinhalte

- Grundlagen Informationssicherheit
- Allgemeine Bedrohungen im militärischen Kontext
- Projektbezogenen Informationssicherheitskonzepte
- Akkreditierung von Waffensystemen
- IT-Grundschutz-Methodik inkl. Praxisbeispiel
- Weiterführende Konzepte und Mechanismen zur Verteidigung

Vortragende

Rudolf Huber Thorsten Slany	MBDA Deutschland GmbH, Schrobenhausen
Dr. Rüdiger Berndt Jochen Veith	Diehl Defence GmbH & Co. KG, Röthenbach a. d. Pegnitz

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Die Teilnehmer werden gebeten einen internetfähigen Laptop zum Seminar mitzubringen. Bitte haben Sie Verständnis, dass wir keine Laptops/PCs zur Verfügung stellen können