LIMES SECURITY

Kursbuch 2026/2027

Limes Academy

Das Angebot der Limes Academy

Wir bieten im Rahmen der Limes Academy Schulungspakete in den Bereichen Security Awareness, OT-Security und Product & Solution Security an.

Security Awareness Training

ab Seite 10

OT-Security Training

ab Seite 20

Product & Solution Security Training

ab Seite 33

Warum Limes Academy?

Alle Trainings werden von unseren erfahrenen Industriesicherheitsexperten abgehalten, die Erfahrung aus einschlägigen Studien und Security Beraterpraxis mitbringen. Sie profitieren damit nicht nur von exzellenten Schulungsinhalten, sondern auch von einem reichhaltigen Erfahrungsschatz. Alle Schulungen beinhalten neben den theoretischen Inhalten auch praktische Übungen, um den Teilnehmern die jeweiligen Themen so greifbar und anschaulich wie möglich zu machen.

+ **Individuelle Schulungsformate**	Unsere Trainings werden in ausgewählten Trainingscentern, an unseren Unternehmensstandorten oder als Online-Format angeboten. Ausgewählte Trainingsinhalte werden auch als E-Learning angeboten. Wir bieten auch individuelle Trainings exklusiv für Ihr Unternehmen an.
+ **Interaktives Training**	Die vermittelten Trainingsinhalte werden durch praktische Übungen gefestigt. Diskussionen regen den Erfahrungsaustausch zwischen den Kursteilnehmern an und fördern das Verstehen des Gelernten.
+ **Schulungsunterlagen**	Die Trainingsunterlagen werden im digitalen Format zur Verfügung gestellt.
+ **Fachkompetenz**	Alle Trainings werden von unseren Sicherheitsexperten abgehalten, die viel Erfahrung aus der Projektpraxis mitbringen.
+ **Aktualität**	Neue Incidents und Security Entwicklungen werden laufend in die Trainingsinhalte integriert. Profitieren Sie vom aktuellsten Security Wissen.
+ **Zertifizierung**	Am Ende des Trainings bekommen Sie eine Teilnahmebestätigung. Bei einigen Kursen besteht die Möglichkeit, durch Prüfungsablegung ein TÜV®-Personenzertifikat zu erlangen.

Über Limes Security

Limes Security ist ein hochprofessionelles Beratungsunternehmen, das sich mit konsequent guter Arbeit innerhalb weniger Jahre eine klare Positionierung am Markt erarbeitet hat. Limes Security steht für Professionalität und Methoden-Know-how auf höchstem Niveau. Unser Ziel ist für unsere Kunden ein angemessenes Sicherheitsniveau zu erreichen, durch herstellerunabhängige Beratung und Weitergabe unseres Experten-Know-hows. Limes Security GmbH ist ein eigentümergeführtes Unternehmen. Das Team von Limes Security besteht aus Top-Experten mit jahrelanger Erfahrung in herausfordernden Projekten. Viele Jahre Erfahrung in der Cybersecurity im industriellen Umfeld stehen im Dienst der Limes Security Auftraggeber.

Unsere Dienstleistungen

Unabhängig davon, ob Windenergie-Weltmarktführer, Softwareentwicklungshaus, Internet-of-Things-Pionier, globaler Player im industriellen Anlagenbau oder städtischer Infrastruktur-Betrieb – Limes Security hat für jeden Betrieb die richtige Dienstleistung:

Sicherer Betrieb von Industrieanlagen
Wir unterstützen Sie bei der Identifizierung technischer und organisatorischer Schwachstellen in Ihrer Organisation, helfen Ihnen beim Aufbau effektiver und effizienter Sicherheitsorganisationen und implementieren geeignete Gegenmaßnahmen.

Sichere Entwicklung von Produkten und Lösungen
Wir helfen Ihnen, Schwachstellen in Ihren Produkten und Lösungen zu identifizieren, unterstützen Sie bei der Einrichtung sicherer Entwicklungspraktiken und coachen Sie bei der langfristigen Behebung von Schwachstellen.

Ausbildung und Zertifizierung von Industriepersonal
Wir ermöglichen Ihnen den Aufbau und die Integration von Security Fähigkeiten in Ihrer Organisation durch hochkarätige Sicherheitsschulungen und die Zertifizierung Ihrer Mitarbeiter.

Kundenspezifische Ausbildungsprogramme
Unsere Kurse können auf Kundenwunsch für unternehmensspezifische Ausbildungsprogramme angepasst werden.

Referenzen

Diese Unternehmen und viele andere setzen auf die Security Kompetenz von Limes Security.

Allgemeine Trainingsinformationen

Sie sind auf der Suche nach dem perfekt zugeschnittenen Training für Ihr Team?

Limes Academy unterstützt Sie gerne bei der Ausbildung Ihrer Mitarbeiter. Wir stellen ein speziell für Ihre Anforderungen zugeschnittenes Trainingsprogramm zusammen. Ausgehend von bereits bestehenden Trainingsinhalten kann das Training individuell an Ihre Wünsche angepasst werden:

Ausrichten der Inhalte und Beispiele auf den Wissensstand Ihrer Mitarbeiter, Ihre Branche und relevante Standards / Vorgaben / Normen sowohl gesetzlicher Natur als auch aus Ihrem Unternehmen.

Anpassen der Trainingsdauer und Durchführungsmodalität (vor Ort, online) auf die Verfügbarkeit der zu schulenden Mitarbeiter.

Anpassen bestehender Übungen bzw. Umsetzung neuer Übungen, die an der spezifischen Kompetenz Ihrer Mitarbeiter ausgerichtet sind.

Senden Sie uns Ihre Anfrage!
https://limessecurity.com/academy/#inhouse-training/

Buchen eines Public Trainings

Um eines unserer Trainings zu buchen, informieren Sie sich bitte über die nächsten öffentlichen Trainingstermine zu Ihrem Thema unter **https://limessecurity.com/academy/trainingsangebot**

Auf der Website können Sie sich dann ganz einfach für unsere öffentlichen Trainings anmelden.

Vorgehen bei einem Inhouse-Training

**Abstimmung der Trainingsinhalte**
Sie wählen Ausbildungsinhalte, die auf Ihre Bedürfnisse zugeschnitten sind.

**Anpassung der Trainings**
Limes Security passt die Übungen und Unterlagen auf die individuell gewählten Inhalte an.

**Auswahl eines Termins**
Sie legen in Absprache mit Limes Security einen Termin für das Training fest.

**Durchführung des Trainings**
Sie legen den Trainingsort und den zeitlichen Rahmen fest.

**Bereitstellen der Schulungsunterlagen**
Limes Security stellt den Schulungsteilnehmern die individuell angepassten Unterlagen bereit.

**Teilnahmezertifikat**
Die Trainingsteilnehmer erhalten am Ende des Trainings ein Teilnahmezertifikat.

**Optionale Zertifizierung**
Am Ende des Trainings kann – falls dies gewünscht wird – für bestimmte Trainings eine offizielle Zertifizierung durch einen unserer Zertifizierungspartner durchgeführt werden.

Wissensvermittlung

Limes Academy bietet Kurse in unterschiedlichen Ausprägungen an, sodass Sie angepasst an Ihren Lernstil am optimalen Training teilnehmen können. Unabhängig davon, ob Sie ein Onlinetraining mit anderen Teilnehmern oder ein persönliches Training in Ihrem Unternehmen bevorzugen: Bei Limes Academy finden Sie ein Lernformat, das Ihren individuellen Anforderungen entspricht.

Inhouse

Das Training wird durch einen Trainer der Limes Academy speziell für Ihr Unternehmen, Ihre Abteilung oder Ihr Team durchgeführt. Das Training findet vor Ort in Ihrem Unternehmen, in einem Trainingscenter oder einem Standort Ihrer Wahl statt.

Inhouse online

Das Training wird durch einen Trainer der Limes Academy speziell für Ihr Unternehmen, Ihre Abteilung oder Ihr Team durchgeführt. Das Training findet online statt und wird mit der Infrastruktur Ihres Unternehmens oder der Infrastruktur von Limes Security abgehalten.

Public

Öffentlich durchgeführte Kurse an ausgewählten Standorten in Österreich und Deutschland, abgehalten von einem Trainer der Limes Academy in deutscher oder englischer Sprache.

Public online

Live mit einem Trainer der Limes Academy wird in einem interaktiven Klassenzimmer das Training durchgeführt. Das Training wird in deutscher oder englischer Sprache abgehalten.

E-Learning

Ausgewählte Lerninhalte können für Ihre firmeninternen Lernplattformen (LMS) in gängigen E-Learning-Formaten (Universal SCORM v1.2 oder SCORM 2004 Formate, xAPI) bereitgestellt werden.

Weitere Details finden Sie ab Seite 16

Haben Sie Fragen?

Falls Sie weitere Informationen zu unserem Trainingsangebot, dem Vorgehen zum Durchführen von Inhouse-Trainings, der Anmeldung zu Public Trainings oder der Erstellung von zugeschnittenen Trainings benötigen, kontaktieren Sie uns gerne direkt.

academy@limessecurity.com

Daniela Weidinger
Trainingsorganisation

Unübertroffene Fachkompetenz

Unser Trainer sind ausschließlich akademisch ausgebildete und erfahrene Security Experten, die über mehrjährige Beratungspraxis in der Industrie oder in der Softwareentwicklung verfügen.

Der Mehrwert für Sie als Teilnehmer:
Sie erhalten zu exzellenten Schulungsinhalten auch einen breit gefächerten Erfahrungsschatz sowie direktes Wissen – aus der Praxis für die Praxis.

Unsere Referenten

Spezialisiert auf

A = Awareness & Compliance Training
O = OT-Security Training
P = Product & Solution Security

Lucas Brandstätter A O

unterstützt in seiner Rolle als IT/OT-Specialist, mit seinem Wissen im ISMS (ISO 27000) und OSMS (IEC 62443) Bereich Unternehmen bei der Einführung von Management-Systemen. Zusätzlich prüft er im Zuge von Risikoanalysen und Penetrationtests Systeme auf Verbesserungpotenzial. Bei Trainings setzt er auf interaktives Feedback.

Thomas Brandstetter A O

ist unser „Breitbandantibiotikum" gegen Security Unwissen. Als Stuxnet Incident Handler und ehemaliger Leiter des Siemens Product-CERTs kennt er OT-Security aus allen Lebenszyklusphasen. Er ist Professor für IT- und Cybersecurity und ist zudem zertifiziert für CISSP, GSEC, GICSP und GRID.

Bettina Wächter A O

behält stets den Überblick und hat gleichzeitig ein Auge für wichtige Details. Mit ihrem Wissen aus ISO 27000, IEC 62443 und NIS-2 sowie ihrer Erfahrung im Arbeiten mit Prozessen schafft sie die organisatorischen Rahmenbedingungen zur Einführung von Managementsystemen. Sie legt großen Wert auf eine nachhaltige Wissensvermittlung.

Peter Eder-Neuhauser A O

zeigt durch die Forschungsschwerpunkte in der Malware-Ausbreitung in IT/OT-Netzen, spezifischen Eindämmungsmaßnahmen und sicherer Architektur die Wichtigkeit von integriertem Risikomanagement, Incident Handling, koordiniertem IT-Governance, Bedrohungs- und Gap-Analysen, Datenschutzfolgeabschätzungen und Awareness.

Nino Fürthauer A O

unterstützt als Penetration Tester Unternehmen dabei, Webapplikationen, Infrastruktur und Systeme besser gegen Angriffe abzusichern. Als Product Owner für die von Limes Security in Kooperation mit TÜV Austria angebotenen Zertifizierungstrainings legt er besonderen Wert auf jedes noch so kleine Detail.

Florian Gerstmayer A O P

war mehrere Jahre als Projektleiter und Embedded-SW-Entwickler tätig, wo er sichere Produkte konzipiert und umgesetzt hat. Dadurch weiß er aus persönlicher Erfahrung, welche Themen im Management angegangen, sowie als Entwickler in einem ganzheitlichen Konzept umgesetzt werden müssen, und vermittelt dies sehr gerne weiter.

Sixtus Leonhardsberger A O P

ist OT-Security Specialist mit Schwerpunkt Penetration Testing von OT-Umgebungen und Embedded Geräten/IoT-Devices. Neben seiner Leidenschaft für technische OT-Security Themen gibt er an die Trainingsteilnehmer auch seine Erfahrungswerte aus Beratungsprojekten zur Absicherung von Netzwerken und Architekturen weiter.

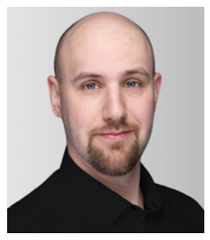
Peter Panholzer A O P

ist Veteran der ersten Stunde bei Industrial Security und sicherer Softwareentwicklung. Er ist zertifizierter ISO-27001-Auditor, Mitglied in der OVE-Arbeitsgruppe zu IEC 62443, Hacker und seit über zehn Jahren Trainer für Secure Coding. Er liebt es, den Teilnehmern knifflige Aufgaben zu stellen und mit den richtigen Security Tipps weiterzuhelfen.

Kerstin Reisinger A O P

ist Offensive Security Certified Professional und Trainerin für Industrial Security. Als langjährige Projektleiterin in komplexen OT-Security Projekten unterstützt sie mit viel technischem Know-how Industrieunternehmen und Energieversorger. Diese Erfahrung bringt sie zur Auflockerung als War Stories und Anekdoten in die Trainings ein.

David Schauer A O



verfügt über ein tiefgreifendes Verständnis von Security aus technischer und organisatorischer Sicht. In seinen Projekten nutzt er das Wissen gezielt, um eine Brücke zwischen technischen Anforderungen und Managementstrategien zu schlagen. Seine Erfahrungen teilt er mit den Teilnehmern, damit diese sicher in beiden Security Welten navigieren können.

Übersicht

100 Security Awareness & Compliance Training

200 OT-Security Training

300 Product & Solution Security Training

100 Security Awareness & Compliance Training

Der Mitarbeiter als Ziel

Ein Großteil der erfolgreich durchgeführten Angriffe nutzt die Schwachstelle Mensch aus, um in die internen Netzwerke einzudringen. Ihre Mitarbeiter müssen verstehen lernen, wo in der täglichen Arbeit Security Risiken lauern – unabhängig davon, ob sie in der Geschäftsführung, in der Produktion oder im Marketing arbeiten.

Trainingsinhalte

Wir vermitteln in unserem erprobten Security Awareness Training jene grundlegende Selbstkompetenz, die Mitarbeiter brauchen, um Risiken unmittelbar zu erkennen und fahrlässiges Verhalten zu vermeiden. Dafür bringt Limes Security Erfahrungen aus Angriffskampagnen, anschauliche Demonstrationen und spannende War-Storys ein. Wir erklären unterhaltsam die essenziellsten Security Regeln, die jeder Mitarbeiter eines modernen Unternehmens wissen sollte, um kein Security Risiko für das eigene Unternehmen zu sein.

AWT.101 IT-Security Awareness

1,5–3 Stunden

alle Mitarbeiter

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 78,– zzgl. MwSt.
Mindestteilnehmeranzahl: 30 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online

IT-Security Awareness

Das IT-Security Awareness Training dient als Grundlage für jeden Mitarbeiter im Unternehmen. Es gilt, ein Grundverständnis für Security zu vermitteln oder bereits vorhandenes Sicherheitswissen wieder aufzufrischen.

Trainingsinhalte

- # Was ist Informationssicherheit?
- # Wer sind die Angreifer?
- # Aktuelle Angriffe, Vorfälle und Hacking-Demo
- # Sichere Verhaltensregeln
  - Umgang mit Programmen, Software und E-Mails
  - Umgang mit Passwörtern und Passwort Policies
  - Umgang mit USB-Sticks und anderen externen Medien
  - Umgang mit eigenen Geräten im Unternehmen (Bring your own Device – BYOD)
  - Umgang mit Informationen
  - Physische Sicherheit
- # Angriffe erkennen und Verdachtsfälle melden
- # Security im privaten Umfeld

Ihr Nutzen

- # Vermittlung von Security Grundverständnis für alle Mitarbeiter
- # Schaffen von Security Bewusstsein bei den Teilnehmern für ein erhöhtes Sicherheitsniveau im eigenen Unternehmen
- # Auffrischen von bereits bekannten Verhaltensregeln für sichere Handlungen im Unternehmen

Anmeldung

Die Anmeldung zum **AWT.101 IT-Security Awareness Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-101/

AWT.102 OT-Security Awareness

1,5–3 Stunden

alle Mitarbeiter

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 78,– zzgl. MwSt.
Mindestteilnehmeranzahl: 30 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online / **E-Learning**

OT-Security Awareness

Das OT-Security Awareness Training dient als Grundlage für jeden Mitarbeiter im OT-Bereich. Es gilt, ein Grundverständnis für Security zu vermitteln oder bereits vorhandenes Sicherheitswissen wieder aufzufrischen. Im Unterschied zum AWT.101 IT-Security Awareness Training werden hier konkrete Beispiele und Verhaltensregeln speziell für den OT-Bereich betrachtet.

Trainingsinhalte

- # Was gehört alles zu Operational Technology (OT)?
- # Wer sind die Angreifer der Industriesysteme?
- # Aktuelle Angriffe, Vorfälle und OT-spezifische Hacking-Demo
- # Sichere Verhaltensregeln für Anlagenpersonal
  - Umgang mit Programmen, Software und E-Mails
  - Umgang mit Passwörtern und Passwort Policies
  - Umgang mit USB-Sticks und anderen externen Medien
  - Physische Sicherheit
- # Angriffe erkennen und Verdachtsfälle melden
- # Top 10 OT-Security Risiken

Ihr Nutzen

- # Vermittlung von Security Grundverständnis für alle Mitarbeiter im OT-Bereich
- # Schaffen von Security Bewusstsein bei den Teilnehmern für ein erhöhtes Sicherheitsniveau im industriellen Betrieb
- # Erkennung und Vermeidung von riskantem Verhalten in den industriellen Anlagen

Anmeldung

Die Anmeldung zum **AWT.102 OT-Security Awareness Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-102/

AWT.103 Zero Downtime: Blackout Edition

2 Stunden

alle Mitarbeiter

Kosten: ab € 4.315,– zzgl. MwSt.
Teilnehmeranzahl: bis zu 80 Teilnehmer

keine Vorkenntnisse notwendig

Inhouse / Inhouse online

Cybersecurity Simulationsspiel Zero Downtime

In Zero Downtime, dem Cybersecurity Simulationsspiel werden Sie zum Verteidigungsteam eines Anlagenbetreibers. Mehrere Teams treten gegeneinander an und lernen dabei spielerisch in der Simulation für die Realität. Dem Simulationsspiel liegt ein ernster Gedanke zu Grunde: Die Teilnehmer lernen aktuelle IT/OT-Bedrohungsszenarien und adäquate Sicherheitskonzepte als Gegenmaßnahmen an vorderster Front kennen. Durch die unmittelbare Einbindung jedes Einzelnen verankern sich die Lerninhalte stark und nachhaltig, gleichzeitig ist Teamwork gefragt.

Am Ende wird jenes Unternehmen zum Sieger gekürt, welches die Herausforderungen am besten bewältigt hat. Das Simulationsspiel wird durch einen Limes Security Experten moderiert und die Ergebnisse werden nach jeder Runde kurz zusammengefasst. Die Teilnehmer spielen gruppenweise entweder online oder an einem Tisch mit Spielbrett in Kombination mit einem Tablet. Für die Teilnahme sind keine besonderen Vorkenntnisse notwendig und das Simulationsspiel ist auch für Einsteiger gut geeignet.

Ihr Nutzen

- Lernen Sie spielerisch wichtige Sicherheitsmaßnahmen und -konzepte kennen.
- Wenden Sie als Teilnehmer wirksame Gegenmaßnahmen gegen Security Bedrohungen an.
- Erfahren Sie, welche Auswirkungen und Konsequenzen bestimmte Sicherheitsmaßnahmen und -konzepte mit sich bringen.
- Werten Sie einen Firmenevent oder eine Konferenz mit einem spielerischen Aspekt auf!

"The 0 Downtime workshop was very effective in engaging and challenging our top management to better understand the cybersecurity risks of our organization and their crucial role for better preparedness and incident response. I believe it was a definite success to bring cybersecurity awareness and culturalization to EDPD. I am a fan of 0 Downtime!" N. Medeiros, EDPD

Anmeldung

Die Anmeldung zum **AWT.103 Zero Downtime: Blackout Edition** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-103/

AWT.104 Cybersecurity Awareness

4 Stunden

alle Mitarbeiter

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 510,– zzgl. MwSt.
Mindestteilnehmeranzahl: 8 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online
Public / Public online

Cybersecurity Awareness

Das Cybersecurity Awareness Training dient als Grundlage für jeden Mitarbeiter im IT/OT-Bereich, um ein Grundverständnis für Security zu vermitteln oder bereits vorhandenes Sicherheitswissen wieder aufzufrischen. Im Unterschied zu rein theoretischen Schulungen werden hier konkrete Beispiele und Verhaltensregeln speziell für den jeweiligen Tätigkeitsbereich der Teilnehmer betrachtet und bestehende Vorurteile in Sachen Cybersicherheit auf deren Wahrheitsgehalt geprüft.

Trainingsinhalte

- Was gehört alles zur Cybersecurity?
- Wer sind die Angreifer der Industriesysteme?
- Aktuelle Angriffe, Vorfälle & IT/OT-spezifische Hacking-Demo
- Sichere Verhaltensregeln:
  - Umgang mit Programmen, Software und E-Mails
  - Umgang mit Passwörtern & Passwort Policies
  - Umgang mit USB Sticks und anderen externen Medien
- Physische Sicherheit
- Angriffe erkennen & Verdachtsfälle melden
- Top 10 Cybersecurity Risiken

Ihr Nutzen

- Vermittlung von Cybersecurity Grundverständnis für alle Mitarbeiter
- Schaffen von Cybersecurity Bewusstsein bei en Teilnehmer für ein erhöhtes Sicherheitsniveau im eigenen Unternehmen
- Auffrischen von bereits bekannten Verhaltensregeln für sichere Handlungen im Unternehmen

Anmeldung

Die Anmeldung zum **AWT.104 Cybersecurity Awareness Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-104/

AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)

2 Stunden

alle Mitarbeiter

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 105,– zzgl. MwSt.
Mindestteilnehmeranzahl: 30 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online / **E-Learning**

Cybersecurity Mitarbeitertraining

Security hat durch NISG (NIS-2) in der heutigen digitalen Welt höchste Priorität bekommen. Ziel des Trainings ist es, dass Mitarbeiter nach Abschluss dieses Trainings nicht nur die Bedeutung von Cybersecurity für das Unternehmen verstehen, sondern auch die Fähigkeiten und das Wissen besitzen, um das Unternehmen besser vor Cyber-Bedrohungen zu schützen. Das „Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)“ wurde daher speziell für Mitarbeiter entwickelt, um diese auf die Herausforderungen in der Cybersecurity vorzubereiten. Mitarbeiter sind ein wesentlicher Schlüssel für die Cybersecurity von Unternehmen. Dieses Training trägt dazu bei, den Anforderungen des NISG (NIS-2) gerecht zu werden. Dieser Kurs dient als Grundlage für jeden Mitarbeiter, der mit Netz- und Informationssysteme in Kontakt kommt und vermittelt ein Grundverständnis für Cyberhygiene. Erfahrene Mitarbeiter können mit diesem Training das bereits vorhandene Security Wissen auffrischen.

Trainingsinhalte

- Was ist Informationssicherheit?
- Was sind Netz- und Informationssysteme?
- Sicherer Umgang mit Informationen
- Wandel der Bedrohungslandschaft
- Was bedeutet „NIS“?
- Wer und was ist betroffen?
- Sichere Verhaltensregeln
  - Umgang mit Passwörtern und Passwort Policies
  - Umgang mit Programmen, Software und E-Mails
  - Umgang mit USB-Sticks und anderen externen Medien
  - Umgang mit eigenen Geräten im Unternehmen
  - Physische Sicherheit
  - Defense-in-Depth Ansatz

Ihr Nutzen

- Schaffen von Security Bewusstsein bei den Teilnehmern für ein erhöhtes Sicherheitsniveau im Unternehmen
- Kenntnisse und Handlungssicherheit in Übereinstimmung mit den durch NISG (NIS-2) geforderten bewusstseinsbildenden Maßnahmen
- Vermittlung von Handlungsempfehlungen für sicheres Arbeiten für alle Mitarbeiter
- Erkennung und Vermeidung von riskantem Verhalten im Unternehmen

Anmeldung

Die Anmeldung zum **AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-111/

AWT.112 NIS-2 Workshop für Management

1 Stunde

Personen in leitenden Funktionen

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 158,– zzgl. MwSt.
Mindestteilnehmeranzahl: 10 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online

NIS-2 Workshop für Management

Der „NIS-2 Workshop für Management“ ist ein speziell konzipierter Workshop, der Personen in leitender Funktion einen umfassenden, aber kompakten Überblick über die persönlichen Verpflichtungen und Haftungen durch NIS-2 bietet. Dieser Workshop unterstützt Führungskräfte in Ihrem Unternehmen die Anforderungen der NIS-2 effizient umzusetzen und eine geeignete Sicherheitskultur zu fördern. Es bietet praktische Einblicke und Strategien, die direkt in der Praxis angewendet werden können.

Trainingsinhalte

Im Workshop werden folgende Themen gemeinsam mit den Teilnehmern behandelt:

- NIS-2-Richtlinie und NIS-2-Gesetz: Erläuterung der rechtlichen Rahmenbedingungen und Anforderungen, die durch die NIS-2-Richtlinie und das NIS-2-Gesetz festgelegt sind.
- Security Kultur: Bedeutung einer starken Sicherheitskultur im Unternehmen und wie diese gefördert werden kann.
- Risikomanagement: Aufgaben im Cybersecurity Risikomanagement und Diskussion geeigneter angemessener technischer, operativer und organisatorischer Risikomanagementmaßnahmen gemäß NIS-2.
- Maßnahmen, Pflichten und Bußgelder: Übersicht über die erforderlichen Maßnahmen zur Einhaltung der NIS-2, die Pflichten der Unternehmen und die möglichen Bußgelder bei Nichteinhaltung.
- Aktuelle Incidents: Analyse aktueller Sicherheitsvorfälle und Diskussion über die daraus resultierenden Lernpunkte.

Ihr Nutzen

- Verständnis der Anforderungen sowie Pflichten aus der NIS-2-Richtlinie und des NIS-2-Gesetzes, um Compliance-Anforderungen des Unternehmens zu erfüllen
- Wissen, wie eine starke Sicherheitskultur im Unternehmen gefördert werden kann
- Praktische Einblicke und Erfahrungswerte zu geeigneten Risikomanagementmaßnahmen als wesentlicher Baustein für die Schaffung einer robusten und widerstandsfähigen digitalen Umgebung im Unternehmen

Anmeldung

Die Anmeldung zum **AWT.112 NIS-2 Workshop für Management** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/awt-112/

E-Learning

Mehrere Kurse der Limes Academy sind als E-Learning-Option für groß angelegte Ausbildungskampagnen und für das Lernen im eigenen Tempo verfügbar.

Awareness	**AWT.102** **OT-Security Awareness**
Compliance	**AWT.111** **Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)**
Foundation	**ICS.201** **OT-Security Fundamentals**

E-Learning-Kurse können ein wesentlicher Baustein für die erfolgreiche Erreichung der Ausbildungsziele Ihres Unternehmens sein. Durch folgende fünf Vorteile unterstützt unser E-Learning Angebot die Weiterqualifikation Ihrer wesentlichsten Assets - Ihre Mitarbeiter:

Relevante und aktuelle Informationen auf Knopfdruck
Aktuelles Security Know-how wird durch interaktives Lernen vermittelt und kann im eigenen Tempo durchgeführt werden, wodurch ein effizientes und flexibles Training ermöglicht wird.

Vermittlung wichtiger Sicherheitskompetenzen
die in großem Umfang von den „Ingenieuren der Zukunft" in einer digitalisierten Industrie benötigt werden.

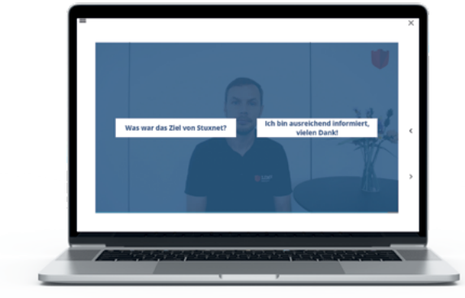
Fragerunden mit Experten
bilden die Möglichkeit, E-Learning mit interaktiven Live-Sitzungen anzureichern

Unternehmensweites Bewusstsein
Entwickelt, um große Gruppen von OT-Mitarbeitern zu unterrichten und sicherzustellen, dass alle OT-Mitarbeiter, einschließlich der Lieferanten, die wichtigsten Sicherheitsaspekte verstehen.

Zeit- und Ortsunabhängiges Lernen
Lerninhalte können für firmeninterne Lernplattformen (LMS) in gängigen E-Learning-Formaten (Universal SCORM v1.2 oder SCORM 2004 Formate, xAPI) bereitgestellt werden.

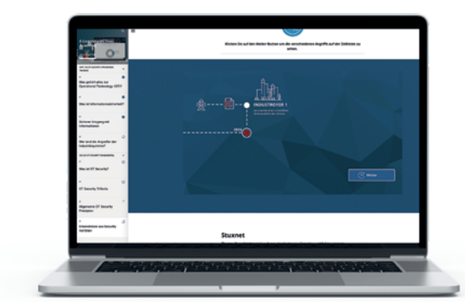
E-Learning-Kurse haben einen schlechten Ruf bekommen. Viele unserer Kunden berichten, dass ihre Mitarbeiter E-Learning-Kurse meiden, weil sie diese häufig als schlecht strukturiert, überholt und wenig ansprechend empfinden. Da E-Learning-Kurse aber ein wertvolles Werkzeug sind, um eine breite Zielgruppe zu erreichen, haben wir unser E-Learning-Angebot an aktuellen Best Practices für die Erstellung wirksamer und ansprechender Lerninhalte ausgerichtet. So werden die Teilnehmer interaktiv und praxisnah durch die Nutzung verschiedener Medienformate und Feedbackmethoden in die Thematik eingebunden.

Interaktive Infografiken bieten vertiefende Informationen durch anklickbare Bereiche und fördern visuelles Lernen.



Interaktive Videos und Szenarien bieten Entscheidungspunkte für personalisierte Lernwege und die Simulation praxisnaher Anwendung.

Interaktive Quizzes fördern die aktive Teilnahme und ermöglichen Selbstbewertung für ein tieferes Verständnis.



Aktuelle Vorfälle und Sicherheitsentwicklungen werden regelmäßig aufgearbeitet und ergänzt.

Neugierig geworden?

Um sich von der Qualität und Effektivität unserer Kurse überzeugen zu können bieten wir hier einen kleinen Einblick in unsere E-Learning-Kurse.

limessecurity.com/de/academy/elearningpreview

Kostenübersicht

Limes Academy bietet verschiedene Pakete und Zusatzoptionen an, um den individuellen Bedürfnissen Ihres Unternehmens gerecht zu werden. Im Folgenden finden Sie eine Aufschlüsselung unserer Angebote. Die Preise gelten pauschal pro Paket unabhängig von der Anzahl der Nutzer - die Preise pro Mitarbeiter dienen nur zur Veranschaulichung.

Standard Paket

Ein E-Learning-Kurs für ein Jahr mit Add-ons kombinierbar

Eckdaten:

- # 1 Jahr Nutzungslizenz
- # Englische oder deutsche Inhalte
- # wahlweise ICS.201 OT-Security Fundamentals oder AWT.102 OT-Security Awareness oder AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)
- # kann mit sämtlichen Add-ons kombiniert werden

Pauschalpreis

€ 0,72 pro Mitarbeiter/Monat* **€ 8.650,–**

All-Access Paket

Alle verfügbaren E-Learning-Kurse für ein Jahr flexibel mit Add-ons kombinierbar.

Eckdaten:

- # 1 Jahr Nutzungslizenz
- # Englische oder deutsche Inhalte
- # ICS.201 OT-Security Fundamentals
- # AWT.102 OT-Security Awareness
- # AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)
- # kann mit sämtlichen Add-ons kombiniert weden

Pauschalpreis

€ 1,11 pro Mitarbeiter/Monat* **€ 13.400,–**

*bei einer Unternehmensgröße von 1.000 Mitarbeiter

Beispiel für ein Unternehmen mit internationaler Reichweite

Ein großes Unternehmen mit 3.500 Mitarbeitern möchte das AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2) nutzen, um sich auf die NIS-2-Konformität vorzubereiten. Es benötigt dafür alle verfügbaren Inhalte in zwei Sprachen, um auch Standorte außerhalb des DACH-Raums bedienen zu können. Zudem soll das Design an das Unternehmens-CI/CD angepasst werden.

- # AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)

Standard Paket

+ Add-on Sprache

+ Add-on Designanpassung

Pauschalpreis

€ 0,41 pro Mitarbeiter/Monat **€ 17.380,–**

Add-ons

Add-ons bieten Ihnen die Möglichkeit, die E-Learning-Kurse zu personalisieren und an die Anforderungen Ihres Unternehmens anzupassen. Flexible Lösungen, von zusätzlichen Sprachen bis hin zu erweiterten Inhaltsanpassungen, stellen sicher, dass Ihre Mitarbeiter das bestmögliche Training erhalten.

Zusätzliche Sprache
Unsere E-Lerning-Kurse sind jeweils in deutscher und englischer Sprache erhältlich.
Pauschalpreis **+ € 5.820,–** 0,48 € pro Mitarbeiter/Monat*

Verlängerung der Lizenz
Die Laufzeit des Pakets kann für eine beliebige Anzahl von Jahren festgelegt werden. Für jedes Jahr wird eine Pauschale erhoben.
Pauschalpreis **+ € 3.880,–** 0,32 € pro Mitarbeiter/Monat*

Designanpassung
Anpassung des Designs an das Corporate Design hinsichtlich Farbe, Schriftart und Logo/Firmenschriftzug.
Pauschalpreis **+ € 2.910,–** 0,64 pro Mitarbeiter/Monat*

Erweiterte Inhaltsanpassung
Einfügen branchenspezifischer Beispiele, Links zu internen Ressourcen oder Ansprechpartnern sowie Anpassung an internes Wording.
Pauschalpreis **+ € 9.730,–** 0,24 € pro Mitarbeiter/Monat*

Live-Sessions und FAQ
Abhaltung vierteljährlicher Live-Sessions mit einem Vortrag zu Cybersecurity Trendthema inkl. FAQ.
Pauschalpreis **+ € 7.760,–** 0,81 € pro Mitarbeiter/Monat*

Beispiel für Unternehmen mit regionaler Ausrichtung

Ein Unternehmen mit etwa 500 Mitarbeitern in Deutschland und Österreich möchte anfangen Cybersecurity Inhalte auch digital anzubieten, anstatt ausschließlich im Vortragsformat. Es möchte daher alle verfügbaren Kurse für 2 Jahre nutzen und benötigt die Inhalte ausschließlich auf Deutsch.

- # ICS.201 OT-Security Fundamentals
- # AWT.102 OT-Security Awareness
- # AWT.111 Cybersecurity Mitarbeitertraining entsprechend NISG (NIS-2)

All-Access Paket

+ Add-on Verlängerung der Lizenz um 1 Jahr

Pauschalpreis

€ 1,44 pro Mitarbeiter/Monat **€ 17.280,–**

200 OT-Security Training

Sichere Digitalisierung für Techniker und Entscheider

Technische Veränderungen im Bereich OT-Security sind neben gesteigerten Sicherheitsanforderungen für Hersteller, Systemintegratoren sowie Betreiber von Industrieanlagen eine neue Herausforderung geworden. Der rasche Wandel inkludiert die Tatsache, dass OT-Security heute völlig anders funktioniert als die bekannte Automatisierungswelt der vergangenen Jahrzehnte.
Limes Security schafft hier Klarheit und generiert Handlungsrichtlinien und Kompetenz für den richtigen Umgang mit Security Themen im industriellen Umfeld.

Trainingsinhalte

Die Trainingsinhalte wurden, basierend auf der Erfahrung aus vielen Industrieprojekten, ausgewählt und zielen auf jene Herausforderungen ab, mit denen die Industrie in der Praxis konfrontiert ist. Unsere Trainings vermitteln dafür sowohl die von industriellem Personal dringend benötigten Security Grundlagen (Foundation) als auch weiterführendes Wissen für Entscheider und Techniker (Advanced) sowie Spezialthemen (Additions). Durch praktische Beispiele und War-Storys unserer Trainer bauen Sie alle benötigten Kompetenzen für die sichere Digitalisierung in der Industrie auf.

Foundation Level

- **ICS.201 OT-Security Fundamentals**
- **ICS.205 Certified OT Security Practitioner (COSP) ***

Advanced Level

- **ICS.211 Certified OT Security Technical Expert (COSTE) ***
- **ICS.212 Certified OT Security Manager (COSM) ***

Additions

- **ICS.221 Assessing OT**
- **ICS.222 OT-Incident Handling Essentials**
- **ICS.223 IEC 62443 Grundlagen, Konzepte & Anwendung**

*** Bei einigen Kursen besteht die Möglichkeit durch Prüfungsablegung ein Zertifikat zu erlangen.**

OT-Security Trainings mit Personenzertifizierung

Technische Veränderungen im Bereich OT-Security sind neben gesteigerten Sicherheitsanforderungen für Hersteller, Systemintegratoren sowie Betreiber von Industrieanlagen eine neue Herausforderung geworden. Der rasche Wandel inkludiert die Tatsache, dass OT-Security heute völlig anders funktioniert als die bekannte Automatisierungswelt der vergangenen Jahrzehnte. Limes Security und TÜV AUSTRIA Akademie schaffen hier Klarheit und vermitteln Handlungsrichtlinien und Kompetenz für den richtigen Umgang mit Security Themen im industriellen Umfeld.

Limes Security bietet dafür ein Personenzertifizierungsschema in Kooperation mit dem TÜV AUSTRIA (https://www.tuv-akademie.at/) an. Die hochwertigen und praxisnahen OT-Security Trainings der Limes Security Academy – vom Practitioner bis zum Manager – sind in drei Modulen aufgebaut und dauern pro Modul 2,5 Tage. Unmittelbar danach kann die Prüfung, abgenommen durch den TÜV AUSTRIA, absolviert werden.

Für wen stellt die Personenzertifizierung einen Mehrwert dar?

Diese Zertifizierung ist perfekt geeignet für Mitarbeiter aus dem industriellen Sektor, die sich für das Thema Security sichtbar weiterqualifizieren wollen, und auch einen entsprechenden Nachweis über Ihre Kenntnisse in diesem Bereich erbringen wollen. **Die Zertifizierung richtet sich damit an Unternehmen aus den Bereichen:** industrielle Komponentenhersteller, produzierende Industrie, Maschinenbauer, Systemintegratoren, Anlagenbetreiber, Energieversorger, Betreiber kritischer Infrastruktur
Personen in der Funktion: Systemintegratoren, Anlagenbetreiber, -planer, -techniker, Instandhaltungsmitarbeiter, Produktionstechniker, Betriebselektriker, Bedienpersonal von Maschinen, Verantwortliche für Anlagen-IT, zukünftige Betriebsführer und Produktionsleiter, Mitarbeiter die direkt mit OT arbeiten, Führungskräfte, deren Mitarbeiter mit OT arbeiten, IT-Mitarbeiter mit Veranwortung für OT-Assets, Mitarbeiter die für die Beschaffung,die Planung oder den Betrieb von OT-Assets verantwortlich sind.
Aufgrund geänderter regulatorischer Anforderungen bzw. Industriesicherheitsstandards (Stichwort NIS-Gesetz, IEC 62443) ist es für industrielle Komponentenhersteller, Systemintegratoren und Anlagenbetreiber immer wichtiger, auch qualifiziertes Personal nachweisen zu können. Das Personenzertifizierungsschema OT-Security hilft dabei.

Personenzertifizierungsschema Übersicht

Training & Prüfung zum Certified OT Security Practitioner TÜV® (COSP)

Level 1: Ausbildungsreihe Operational Technology Security abgebildet durch den Kurs ICS.205 Certified OT Security Practitioner (COSP)
Voraussetzungen: Keine Vorkenntnisse erforderlich, Grundlagenkenntnisse der Informationssicherheit sind nützlich

Training & Prüfung zum Certified OT Security Technical Expert TÜV® (COSTE)

Level 2: Ausbildungsreihe Operational Technology Security abgebildet durch den Kurs ICS.211 Certified OT Security Technical Expert (COSTE)
Voraussetzungen: Abgeschlossene Ausbildung inkl. Zertifizierung zum „Certified OT Security Practitioner TÜV® (COSP)“ der TÜV AUSTRIA Akademie oder eines gleichwertigen Lehrgangs oder eine einschlägige mind. 6-monatige, durchschnittlich mind. 20 Wochenstunden umfassende Berufserfahrung

Training & Prüfung zum Certified OT Security Manager TÜV® (COSM)

Level 2: Ausbildungsreihe Operational Technology Security abgebildet durch den Kurs ICS.212 Certified OT Security Manager (COSM)
Voraussetzungen: Abgeschlossene Ausbildung inkl. Zertifizierung zum „Certified OT Security Practitioner TÜV® (COSP)“ der TÜV AUSTRIA Akademie oder eines gleichwertigen Lehrgangs oder eine einschlägige mind. 6-monatige, durchschnittlich mind. 20 Wochenstunden umfassende Berufserfahrung

Details zur Zertifizierung

Limes Security hat mit der TÜV AUSTRIA Akademie einen verlässlichen und starken Partner im Bereich der Personenzertifizierung gefunden. Denn TÜV AUSTRIA ist eine international tätige Zertifizierungsstelle für die Bereiche Personen-, Produkt und Systemzertifizierungen. Diverse Akkreditierungen, behördliche Ermächtigungen und gewerberechtliche Befugnisse sind die Grundlage für weltweit anerkannte Zertifikate. Jedes Zertifizierungsverfahren von Personen erfüllt die strengen Forderungen der internationalen Norm ISO/IEC 17024. Personenzertifikate des TÜV AUSTRIA schaffen Vertrauen und bieten Ihnen einen klaren Vorteil in der Berufswelt.

Prüfungsablauf

Die Prüfung im Rahmen der OT-Security Personenzertifizierung wird in einer eigens dafür von TÜV AUSTRIA bereitgestellten Software durchgeführt. Benötigt werden dafür ein Lichtbildausweis sowie bei der Online-Abnahme eine Kamera.

Für die Prüfung stehen 60 Minuten zur Verfügung, um ingesamt 30 Fragen im Single-Choice-Modus zu beantworten. Auf die ausgestellten Trainingsunterlagen darf während der Prüfung zurückgegriffen werden.

Nach positivem Abschluss der Prüfung kann mit dem TÜV AUSTRIA Personenzertifikat bestätigt werden, dass ein bestimmtes Wissen kompetent angewendet und umgesetzt werden kann.

Bei Public- und Inhouse-Trainings kann die Zertifizierung unmittelbar im Anschluss an den letzten Trainingstag abgelegt werden.

Kosten

In der Zertifizierungsgebühr ist die Ausstellung eines Zertifikats inkludiert. Zweitzertifikate, z. B. in Englisch, werden separat verrechnet. Anderssprachige Zertifikate können gerne auf Anfrage ausgestellt werden. Jede Prüfung, bzw. jeder Prüfungsteil darf einmal im Rahmen eines der nächsten Prüfungstermine entsprechend der freien Plätze kostenlos wiederholt werden. Extratermine werden nach Aufwand verrechnet.

Gültigkeit

Damit Ihr Wissen immer am Stand der technischen und inhaltlichen Entwicklungen bleibt, ist die Gültigkeit Ihres Zertifikates zeitlich begrenzt. Die TÜV AUSTRIA Personenzertifikate für OT-Security sind drei Jahre gültig.

Rezertifizierung

Aktuelle Informationen zur Rezertifizierung finden Sie hier: **https://limessecurity.com/de/academy/rezertifizierung/**

Digital Badges

Zusätzlich zu den klassischen Personenzertifikaten sind auch digitale Badges erhältlich. Gemeinsam mit Credly bieten wir digitale Versionen unserer Zertifizierungen an. Verwenden Sie Ihre Limes Academy Badges für Ihre E-Mail-Signatur, Ihren digitalen Lebenslauf und auf Social Media, um Ihre OT-Security Expertise sichtbar zu machen. Jeder digitale Badge enthält verifizierte Metadaten, die Ihre Qualifikation und den für den Erwerb notwendigen Prozess beschreiben.

Welche Vorteile haben digitale Badges von Limes Academy?

- Einfache Verwaltung, Freigabe und Verifizierung Ihrer OT-Security Qualifikation
- Erhöhte Glaubwürdigkeit durch transparenten Verifizierungs-Prozess
- Digitale Badges dienen Arbeitgebern und Peers als eindeutiger Nachweis

Jetzt Badge beantragen: https://limessecurity.com/de/academy/digitale-badges-beantragen/

ICS.201 OT-Security Fundamentals

3 Stunden

alle Mitarbeiter

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 346,– zzgl. MwSt.
Mindestteilnehmeranzahl: 15 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online / **E-Learning**

OT-Security Fundamentals

Das Training „ICS.201 OT-Security Fundamentals“ ist der perfekte Einstiegskurs in das Thema OT-Security. Im Kurs wird Verständnis für das Thema OT-Security aufgebaut sowie ein Überblick vermittelt, wie damit umzugehen ist. Die Teilnehmer lernen basierend auf realen Vorfällen, praktischem Wissen aus OT-Projekten, Fallstudien sowie Erkenntnissen aus OT-Security Tests, wie sie den Security Ist-Stand Ihrer OT-Umgebung verstehen und hinterfragen können.

Trainingsinhalte

Einführung:
Was ist OT-Security und warum ist sie wichtig
Erkenntnisse aus OT-Security Incidents
- Stuxnet, Triton, Colonial Pipeline, Solar Winds, Industroyer 1 & 2
- Alternativ: branchenspezifische bzw. unternehmensspezifische Incidents
- Wandel der Bedrohungslandschaft

Wichtige Security Aspekte im OT-Umfeld
- Herausforderungen
- Störung der Verfügbarkeit
- Probleme mit der Integrität
- Verlust von Vertraulichkeit
- Häufige Security Probleme in OT-Umgebungen

Strategien zur Risikominderung für Anlageningenieure, Instandhalter und Betriebspersonal
- Nutzen von Security Anforderungen für Anlagen
- Allgemeine Security Prinzipien
- Organisatorische Maßnahmen
- Maßnahme für Netzwerk- und Kommunikationssicherheit
- Maßnahmen zur Absicherung von Komponenten

Abschluss
- Verhalten bei Vorfällen
- Weitere Quellen für Informationen
- Schlussfolgerungen und wichtige Punkte

Anmeldung

Die Anmeldung zum **ICS.201 OT-Security Fundamentals Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/ics-201/

ICS.205 Certified OT Security Practitioner (COSP)

3 Tage

eigenes Notebook notwendig

keine Vorkenntnisse notwendig

Schulungsunterlagen/Teilnahmezertifikate
Zertifizierungsmöglichkeit!

Kosten/Teilnehmer: € 3.160,– zzgl. MwSt. (inkl. Zertifizierungsprüfung)
Mindestteilnehmerzahl: 8 Personen

Inhouse / Inhouse online
Public / Public online

» **Wenn Sie für dieses Training nur die Zertifizierung absolvieren möchten, nehmen Sie bitte mit uns Kontakt auf.**

Applied OT-Security

Das Training „ICS.205 Certified OT Security Practitioner (COSP)“ ist der ideale Kurs für alle Personen, die sich auf eine Rolle oder Funktion mit OT-Security Verantwortung angemessen vorbereiten wollen. Das Training vermittelt wesentliches Know-how der OT-Security, gibt einen Überblick der gängigen Standards und stellt konkrete Maßnahmen für einen sicheren Betrieb von Industriesystemen vor. Damit werden vorhandene Fähigkeiten aus den Bereichen Instandhaltung, Automatisierungstechnik, Mess-, Steuerungs- und Regelungstechnik gezielt ergänzt, um auch die Security Perspektive in vernetzten Industriesysteme einnehmen zu können.

Trainingsinhalte

Tag 1

Einführung in Operational Technology (OT)
  - IT-Sicherheitsziele
  - Einführung in Steuerungsanlagen
  - OT-Komponenten und Terminologie
  - OT-Incidents
IT-Grundlagen
  - Netzwerkprotokolle
  - Krypto-Auffrischung
  - Grundlagen der Netzwerksicherheit
  - Sichere Netzwerkprotokolle

Tag 2

IT- vs. OT-Security
  - Safety vs. Security
  - Charakteristiken von OT-Systemen vs. IT-Systemen
Security Bedrohungen und Angriffsvektoren
  - OT-Angreifer
  - OT-Angriffsvektoren
  - OT-Bedrohungen
OT-Security Standards und Vorschriften
  - NIS-Richtlinie
  - IEC 62443
  - ISO 27000 & ISO 27019
  - NIST 800-82 und CSF
  - und viele mehr

Tag 3

Erprobte Security Maßnahmen für OT
  - Defense in Depth
  - Organisatorische Sicherheitsmaßnahmen
  - Security Assessments und Reviews
  - Konfigurationsmanagement
  - Netzwerk- und Kommunikationssicherheit
  - Komponentensicherheit
  - Benutzer- und Identitätsmanagement

Das Training ist ideal geeignet für …

Systemintegratoren
Anlagenbetreiber, -planer, -techniker
Instandhaltungsmitarbeiter
Produktionstechniker
Betriebselektriker
Bedienpersonal von Maschinen
Verantwortliche für Anlagen-IT
zukünftige Betriebsführer und Produktionsleiter
Mitarbeiter, die direkt mit OT arbeiten
Führungskräfte, deren Mitarbeiter mit OT arbeiten
IT-Mitarbeiter mit Veranwortung für OT-Assets
Mitarbeiter, die für die Beschaffung,die Planung oder den Betrieb von OT-Assets verantwortlich sind

Die Teilnehmer sollten nach der Ausbildung …

ein sicheres Gefühl im persönlichen Umgang mit OT-Security haben.
ein grundlegendes Verständnis von OT-Technologien und Begrifflichkeiten haben.
grundlegende Kenntnisse über OT-Security Standards und deren Anwendungsbereiche haben.
die wichtigsten Sicherheitsmaßnahmen für den OT-Bereich kennen.
in ihrem Verantwortungsbereich den richtigen Beitrag zum Schutz des industriellen Betriebs leisten können.

Certified OT Security Practitioner TÜV® (COSP)

Anmeldung

Die Anmeldung zum **ICS.205 Certified OT Security Practitioner (COSP)** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/ics-205/

ICS.211 Certified OT Security Technical Expert (COSTE)

3 Tage

eigenes Notebook notwendig

Kosten/Teilnehmer: € 3.470– zzgl. MwSt. (inkl. Zertifizierungsprüfung)
Mindestteilnehmeranzahl: 8 Personen

ICS.205 Certified OT Security Practitioner (COSP) Training oder anderes gleichwertiges Training

Inhouse / Inhouse online
Public / Public online

Schulungsunterlagen/Teilnahmezertifikate
Zertifizierungsmöglichkeit!

» **Wenn Sie für dieses Training nur die Zertifizierung absolvieren möchten, nehmen Sie bitte mit uns Kontakt auf.**

OT-Security Advanced: Technical OT-Security

Das Training „ICS.211 Certified OT Security Technical Expert (COSTE)" zielt darauf ab, bereits vorhandenes Wissen von Personen mit einschlägiger Berufserfahrung in IT- und OT-Security weiter zu festigen und zu vertiefen. Das Training mit technischem Fokus vermittelt das benötigte Verständnis von eingesetzten Protokollen und Komponenten sowie tiefgehenden Security Kenntnissen zu Bedrohungen, aktuellen Angriffskampagnen und dem Einsatz von technischen Schutzmaßnahmen. Das Training befähigt die Teilnehmer die richtigen Entscheidungen bezüglich angemessener technischer Security Maßnahmen und Security Technologien zu treffen bzw. vorzubereiten und so das Sicherheitsniveau von Anlagennetzen mittels erprobten Methoden und Technologien zu erhöhen.

Trainingsinhalte

Tag 1

Einführung
  - OT-Threat Landscape
  - Beschaffung eines sicheren Systems
  - IEC 62443 Risikoanalyse
OT-Protokolle
  - Gängige drahtgebundene und drahtlose OT-Protokolle
  - OT-Protokolle auf technischer Ebene verstehen
  - Drahtlose Protokolle in OT-Umgebungen
  - Absicherung von Industrieprotokollen
  - Netzwerk- und Protokollanalyse mit Wireshark

Tag 2

Netzwerkbasierte Angriffe
  - MAC-Spoofing
  - Denial-of-Service-Angriffe
  - Netzwerk-Sniffing
  - Protokoll-Spoofing
  - Man-in-the-Middle-Angriffe
Verbesserung von OT-Network Security
  - Netzwerksegmentierung
  - Einsatz von Firewalls in OT-Netzwerken

Tag 3

Anwendung von Security Maßnahmen in der OT
  - Security Requirements und deren Implementierung
  - User Management
  - Credential Management
  - Host Hardening
  - System Monitoring und Network Detection
  - Anomaly und Threat Detection
  - Remote Access
  - Backup und Recovery
  - OT-Security Market Guide
  - OT-Security Trends
Final Challenge

Das Training ist ideal geeignet für ...

Systemintegratoren
Anlagenbetreiber, -planer, -techniker
Instandhaltung
Produktionstechniker
Verantwortliche für Anlagen-IT
zukünftige Betriebsführer und Produktionsleiter
Mitarbeiter, die für die Beschaffung, die Planung der den Betrieb von OT-Assets verantwortlich sind
IT-Mitarbeiter mit Veranwortung für OT-Assets

Die Teilnehmer sollten nach der Ausbildung ...

bereits vorhandenes Wissen in IT- und OT-Security weiter gefestigt und vertieft haben.
ein grundlegendes Verständnis von OT-Übertragungstechnologien und spezifischen Protokollen besitzen.
unterschiedliche Netzwerkschutzmaßnahmen der OT anhand gängiger Angriffe verstanden haben.
das Vorgehen zur Partitionierung und Zonierung einer Architektur kennengelernt haben.
einen Einblick in die Nutzung von Monitoring-Systemen gegen Angreifer gewonnen haben.
gelernt haben, wie Sicherheitsmaßnahmen im OT-Betrieb technisch umgesetzt werden können.

Self-Assessment Questionnaire

Unser Self-Assessment Questionnaire gibt Ihnen eine erste Einschätzung, ob Sie für das Certified OT Security Technical Expert Training geeignet sind. Infos dazu:
https://limessecurity.com/de/academy/ics-211/#costequestionnaire

Anmeldung

Die Anmeldung zum **ICS.211 Certified OT Security Technical Expert (COSTE)** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

Certified OT Security Technical Expert TÜV® (COSTE)

https://limessecurity.com/academy/ics-211/

ICS.212 Certified OT Security Manager (COSM)

3 Tage

eigenes Notebook notwendig

Kosten/Teilnehmer: € 3.470,- zzgl. MwSt. (inkl. Zertifizierungsprüfung)
Mindestteilnehmeranzahl: 8 Personen

ICS.205 Certified OT Security Practitioner (COSP) Training oder anderes gleichwertiges Training

Inhouse / Inhouse online
Public / Public online

Schulungsunterlagen/Teilnahmezertifikate
Zertifizierungsmöglichkeit!

» **Wenn Sie für dieses Training nur die Zertifizierung absolvieren möchten, nehmen Sie bitte mit uns Kontakt auf.**

OT-Security Advanced: Management

Das Training „ICS.212 Certified OT Security Manager (COSM)" vermittelt Betriebsverantwortlichen, Projekt- und Produktionsleitern sowie generell Entscheidern das erforderliche Wissen zur Umsetzung von Security im industriellen Betrieb. Teilnehmer lernen dabei alle notwendigen Fähigkeiten, um Gefahren frühzeitig zu erkennen, das Security Niveau zu erhöhen und Security Schwachstellen nachhaltig zu vermeiden. Der Fokus liegt dabei auf organisatorischen Themen und Prozessmanagement, zusätzlich wird jedoch auch auf technische Einflussfaktoren eingegangen, die die Teilnehmer für kommende Security Entscheidungen besser rüsten.

Trainingsinhalte

Tag 1
- Einführung
  - Übersicht, Standards und Frameworks
  - Tabletop Exercise
- Govern
  - Security Governance and Program Management
  - Rollen und Verantwortlichkeiten
  - System under Consideration
  - Supply Chain Risk Management
- Identify
  - Improvement
  - Asset Inventory
  - Risk Management

Tag 2
- Protect
  - Defense in Depth
  - Netzwerksegmentierung und Zonierung
  - Remote Access
  - Systems Security
  - Patch Management
  - Identity und Access Management
  - Security Awareness
- Detect
  - Logging und Monitoring
  - Anomaly Detection
  - Vulnerability Assessment

Tag 3
- Respond
  - Incident Handling Lifecycle
  - Post Incident Activities
- Recover
  - System Availability
  - Recovery Planning
  - Backup

Das Training ist ideal geeignet für ...

- Systemintegratoren
- Anlagenbetreiber, -planer, -techniker
- Instandhaltung
- Produktionstechniker
- Verantwortliche für Anlagen-IT
- zukünftige Betriebsführer und Produktionsleiter
- Mitarbeiter, die für die Beschaffung, die Planung oder den Betrieb von OT-Assets verantwortlich sind
- IT-Mitarbeiter mit Veranwortung für OT-Assets

Self-Assessment Questionnaire

Unser Self-Assessment Questionnaire gibt Ihnen eine erste Einschätzung, ob Sie für das Training zum Certified OT Security Manager geeignet sind.
Infos dazu:
https://limessecurity.com/de/academy/ics-212/#cosmquestionnaire

Anmeldung

Die Anmeldung zum **ICS.212 Certified OT Security Manager (COSM)** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

Die Teilnehmer sollten nach der Ausbildung ...

- ihre verantworteten Betriebsbereiche sicher führen und Risiken bewerten können.
- bestehendes Wissen über OT-Security und dazugehörige Standards aufgefrischt und vertieft haben.
- ein grundlegendes Verständnis für das Risk Assessment Vorgehen aufgebaut haben.
- Möglichkeiten zur Asset Discovery und Klassifizierung von Komponenten verstehen.
- eine ganzheitliche Sicht der Security Prozesse entwickelt haben.
- Response Pläne definieren und definierte Kommunikationsstrategien für das Vorfallsmanagement etablieren können.

Certified OT Security Manager TÜV® (COSM)

https://limessecurity.com/academy/ics-212/

ICS.221 Assessing OT

1 Tag | Techniker | eigenes Notebook notwendig | Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 805,– zzgl. MwSt.
Mindestteilnehmeranzahl: 10 Personen | ICS.211 Certified OT Security Technical Expert (COSTE) | Inhouse / Inhouse online

OT-Security Additions: Assessing OT

Das Training „ICS.221 Assessing OT“ vermittelt Teilnehmern jene Grundlagen, um Security Tests in Industrieanlagen professionell durchführen zu können. Welche Tools sollten für welchen Anwendungsfall eingesetzt werden? Welche Testfälle sind intrusiv und damit für OT weniger geeignet? Welche Information ist überhaupt im Rahmen eines OT-Security Audits relevant? Teilnehmer profitieren in diesem Kurs insbesondere von der jahrelangen Erfahrung der Experten der Limes Security bei der Durchführung von Security Assessments im Industrieumfeld.

Trainingsinhalte

- # Underground Economy
- # Anforderungen an Sicherheitstest aus IEC 62443 und ISO 27001
- # OT-Asset Discovery
- # Überprüfung von Benutzern und Berechtigungen
- # Konfigurationsreview von OT-Systemen
- # Überprüfung von Patch- und Softwareständen
- # Überprüfung des Perimeterschutzes
- # Vorgehen bei einem OT-Security Test
- # Test der BSI ICS Top 10
- # Einsatz und Parametrierung von Testwerkzeugen für Produktivumgebungen

Ihr Nutzen

- # Netzwerke und Systeme mit den Augen eines Angreifers betrachten und potenzielle Angriffsvektoren und Sicherheitsprobleme identifizieren.
- # Kenntnisse, was bei einer Sicherheitsüberprüfung im industriellen Umfeld beachtet werden muss.
- # Wissen, wie die Ergebnisse aus einer Sicherheitsüberprüfung zu einem erhöhten Sicherheitsniveau führen können.

Anmeldung

Die Anmeldung zum **ICS.221 Assessing OT-Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/ics-221/

ICS.222 OT-Incident Handling Essentials

1 Tag | Techniker und Entscheider | eigenes Notebook notwendig | Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 805,– zzgl. MwSt.
Mindestteilnehmeranzahl: 10 Personen | ICS.201 OT Security Fundamentals oder ICS.205 Certified OT Security Practitioner (COSP) empfohlen | Inhouse / Inhouse online

OT-Security Additions: Incident Handling Essentials

Das Training „ICS.222 OT-Incident Handling Essentials“ vermittelt Teilnehmern die notwendigen Grundlagen, um sich auf Security Incidents im industriellen Umfeld vorzubereiten. Dabei werden die wichtigsten technischen und organsatorischen Vorbereitungen diskutiert, sowie „DOs and DON'Ts“. Dieser Kurs ist insbesondere für Anlagenbetreiber, Integratoren und Dienstleister interessant, die sich für den Ernstfall vorbereiten möchten, um Schaden durch Virenbefälle, Ransomware oder Hacking leichter abwenden zu können.

Trainingsinhalte

- # Einführung zu Incident Handling
  - Grundlagen und Begriffe
  - OT-Incident Handling
  - Incident Handling Lifecycle
- # Vorbereitung
  - Maßnahmen und Definitionen
  - Incident Report Template
- # Erkennung und Analyse
  - Typische Arten von Indikatoren
  - Quellen für Alerts
  - MITRE ATT&CK
  - Hands-on: Analyse eines OT-Incidents
- # Containment, Eradication und Recovery
- # Post-Incident Activities

Ihr Nutzen

- # Verbesserung der Fähigkeit Security Incidents als solche rechtzeitig zu erkennen
- # Verständnis für die richtige Behandlung von Incidents in der OT sicherstellen
- # Wissen, welche Vorbereitungen im unternehmenseigenen OT-Betrieb für Security Incidents zu setzen sind

Anmeldung

Die Anmeldung zum **ICS.222 OT-Incident Handling Essentials** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/ics-222/

ICS.223 IEC 62443 Grundlagen, Konzepte & Anwendung

1 Tag

interaktiver Workshop

kein Notebook notwendig

Schulungsunterlagen und Teilnahmezertifikate

Kosten/Teilnehmer: € 805,– zzgl. MwSt.
Mindestteilnehmeranzahl: 10 Personen

keine Vorkenntnisse notwendig

Inhouse / Inhouse online

IEC 62443: Grundlagen, Konzepte & Anwendung

In diesem Mix aus interaktiven Workshop und klassischem Training werden den Teilnehmern die wichtigsten Begriffe und grundlegenden Konzepte der Normenreihe IEC 62443 vermittelt. In Gruppendiskussionen und Fragerunden kann dabei auf die individuellen Bedürfnisse der Teilnehmer direkt eingegangen werden.
Die Experten der Limes Security bringen dabei auch Praxiserfahrung aus Jahren der Anwendung der unterschiedlichen Normenteile in unterschiedlichen Industrien mit, welche Schwierigkeiten und Diskussionen dabei immer wieder aufkommen, und welche Herangehensweisen einen erfolgreichen Umgang mit den unterschiedlichen Normen ermöglichen. In praktischen Übungen werden außerdem Konzepte wie Zones & Conduits oder Security Levels weiter vertieft.

Trainingsinhalte

- # Überblick IEC 62443
  - Aufbau der Normenreihe
  - Rollen: Betreiber, Integrator, Hersteller
  - Zertifizierungsmöglichkeiten
- # Grundbegriffe & Konzepte
  - Anforderungen, Security Levels & Maturity Levels
  - Zones & Conduits
  - Compensating Countermeasures
- # Risikoanalyse nach IEC 62443-3-2
  - System under Consideration
  - Grobe und detaillierte Risikoanalyse
  - Ableitung von Ziel-Security-Levels
- # Normenteile im Detail
  - Aufbau der Normenreihe
  - 3-3 / 4-2: technische Security-Anforderungen
  - 4-1 Secure Development Lifecycle
  - 2-1 Security Program für Betreiber
  - 2-4 Anforderungen an Integratoren & Service Provider
- # Einordnung & Anwendung
  - Zusammenspiel mit ISO 27001
  - Bedeutung von Zertifikaten
  - Praxisbeispiele und Übungen

Anmeldung

Die Anmeldung zum **ICS.223 IEC 62443 Grundlagen, Konzepte & Anwendung** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/ics-223/

Ihr Nutzen

- # Effiziente Einführung eines großen Personenkreises in das Thema IEC 62443 möglich
- # Interne Fragestellungen können im Beisein eines IEC-62443-Experten der Limes Security bereits im Kurs diskutiert werden
- # Anpassung der Trainingsinhalte bzw. Fokuspunkte, um ein Customizing an das eigene Unternehmen vorzunehmen

Sichere Produkte & Lösungen durch Know-how-Vorsprung

Wie können Security Schwachstellen von Anfang an vermieden werden? Nur durch geeignete Ausbildung und Verbesserung des Security Know-hows der Entwickler und Projektmitglieder. Wir vermitteln die „DOs and DON'Ts" in Theorie und in praktischen Übungen. In den Product and Solution Security Trainings vermitteln erfahrene Trainer der Limes Security das Wissen, wie Angreifer vorgehen und welche Maßnahmen am besten dagegen schützen.

Trainingsinhalte

Das Security Testing Training lehrt den Teilnehmern den Blickwinkel eines Angreifers einzunehmen, wodurch sie effizient Schwachstellen in ihren Produkten identifizieren können. Das Training „PSS.311 Sichere Entwicklungsprozesse für OT und (I)IoT" vermittelt den Teilnehmern, wie mit Hilfe von Normen Security in die Softwareentwicklung integriert werden kann, um ihre Produkte nachhaltig sicher zu machen.

Im Training Sichere Embedded & (I)IoT-Produkte liegt der Fokus in der richtigen und ganzheitlichen Umsetzung von Security um konform zu Gesetzen und Verordnungen zu sein. Dabei sind alle Trainings mit praktischen Übungen versehen, die sowohl die Angreifer als auch die Verteidigerseite beleuchten, wodurch ein vielschichtiges Bild vermittelt wird.

Secure Development Lifecycle

- **PSS.311**
  Sichere Entwicklungsprozesse für OT und (I)IoT
- **PSS.312**
  Cyber Resilience Act (CRA) für Hersteller von Maschinen und Geräten

Security Testing

- **PSS.321**
  Security Testing Foundation

Security Engineering

- **PSS.331**
  Sichere Embedded & (I)IoT-Produkte

PSS.311 Sichere Entwicklungsprozesse für OT und (I)IoT

2,5 Tage

Kosten/Teilnehmer: € 2.025,– zzgl. MwSt.
Mindestteilnehmeranzahl: 8 Personen

Entwicklungsleiter, Projektleiter, Produktmanager, Entwickler, Qualitätsmanager, Architekten, Tester, CE- Beauftragte

kein Notebook notwendig

keine Vorkenntnisse notwendig

Schulungsunterlagen und Teilnahmezertifikate

Inhouse / Inhouse Online
Public / Public Online

Produkte konform zu Cyber Resilience Act, Maschinenverordnung, IEC 62443-4-1 und Co. entwickeln

Wer die Security und damit die Qualität seiner Produkte nicht dem Zufall überlassen möchte, der muss einen proaktiven Zugang wählen. Nur durch die Integration von Security in die Entwicklungsprozesse und durch eine Organisation, die mit dem Thema professionell umzugehen weiß, entstehen hochwertige, dem Markt gerechte Produkte. Das Training „Sichere Entwicklungsprozesse für OT und (I)IoT“ vermittelt den Teilnehmern, wie Security in die Produktentwicklung integriert werden kann, um ihre Produkte nachhaltig sicher zu machen.

Trainingsinhalte

Tag 1

Überblick Regularien
- Maschinenverordnung
- Funkanlagen-Richtlinie (RED)
- Cyber Resilience Act (CRA)

Überblick Normen
- IEC 62443 Normenreihe Allgemein
- IEC 62443-4-1 Prinzipien und Anforderungen

Security Management
- Produktklassifizierung
- Security Organisation
- Security Trainings
- Integritätsschutz
- Absicherung der Entwicklungsumgebung
- Auswahl sicherer Komponenten

Tag 2

Spezifikation von Security Requirements
- Produkt Sicherheits-Umfeld
- Safety & Security
- Bedrohungsanalyse

Sicheres Design & Entwicklung
Security Verification & Validation Testing

Tag 3

Schwachstellen Management
Security Update Management
Security Dokumentation

Das Training ist ideal geeignet für Hersteller von …

OT-Komponenten
Maschinen
IoT-Produkten
Embedded Lösungen

Die Teilnehmer sollten nach der Ausbildung …

den Zusammenhang von Safety und Security verstehen.
regulatorische und normative Anforderungen kennen und umsetzen können.
verstehen, was sichere Produktentwicklung umfasst und was dafür in der Organisation notwendig ist.
verstehen, was ein Threat Model ist und was zur Erarbeitung eines solchen notwendig ist.
geeignete Methoden und passende Maßnahmen zur Integration von Security in den Produktentwicklungsprozess kennen.
nützliche Tools zur Überprüfung und Verbesserung der Produktsicherheit kennen.
ständigen Herausforderungen wie Umgang mit Legacy Code, Updates von Dritt-Komponenten oder Kommunikation von Schwachstellen begegnen können.

Anmeldung

Die Anmeldung zum **PSS.311 Sichere Entwicklungsprozesse für OT und (I)IoT Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/trainings/pss-311/

PSS.312 Cyber Resilience Act (CRA) für Hersteller von Maschinen und Geräten

1 Tag

Kosten/Teilnehmer: € 940,– zzgl. MwSt.
Mindestteilnehmeranzahl: 10 Personen

Entwicklungsleiter, Projektleiter, Produktmanager, Entwickler, Qualitätsmanager, Architekten, Tester, CE- Beauftragte

eigenes Notebook notwendig

keine Vorkenntnisse notwendig

Schulungsunterlagen und Teilnahmezertifikate

Inhouse / Inhouse Online
Public / Public Online

CRA-Anforderungen für Maschinen und Geräte praxisnah umsetzen

Der Cyber Resilience Act stellt neue Anforderungen an Hersteller von Maschinen, Anlagen und elektrischen Geräten. Im Training erfahren die Teilnehmer, welche Produkte betroffen sind und wie regulatorische CE-Anforderungen mit technischen und organisatorischen Security-Maßnahmen verbunden werden.

Praxisnah wird vermittelt, wie eine Security-Risikoanalyse durchgeführt, Security by Design in Entwicklungsprozesse integriert und ein wirksames Schwachstellenmanagement aufgebaut werden kann. Auch Dokumentationspflichten, Sicherheitsupdates und die Anforderungen an die Konformitätsbewertung werden behandelt.

Trainingsinhalte

Cyber Resilience Act und CE-Kennzeichnung
- Maschinenverordnung
- Funkanlagen-Richtlinie (RED)
- Cyber Resilience Act (CRA)

Security-Risikoanalyse & sichere Entwicklung
- Bedrohungs- und Security-Risikoanalysen
- Security by Design, IEC 62443 und Secure Coding
- Sichere Architekturen, Entwicklungsprozesse und Tests

Schwachstellenmanagement & Dokumentation
- Schwachstellenmanagement, SBOM und Sicherheitsupdates
- Sichere Fernwartung und technische CRA-Anforderungen
- Technische Dokumentation und Konformitätserklärung

Das Training ist ideal geeignet für Hersteller von …

OT-Komponenten
Maschinen
IoT-Produkten
Embedded Lösungen

Die Teilnehmer sollten nach der Ausbildung …

einschätzen, welche Produkte unter den Cyber Resilience Act fallen.
CRA, CE-Kennzeichnung, RED und Maschinenverordnung einordnen.
Security-Risiken systematisch identifizieren und bewerten.
Security by Design in Entwicklungsprozesse integrieren.
technische und organisatorische Security-Maßnahmen ableiten.
Schwachstellen-, Update- und SBOM-Prozesse strukturieren.
Anforderungen an Konformitätsbewertung und Dokumentation umsetzen.
Rollen und Verantwortlichkeiten im Unternehmen definieren.

Anmeldung

Die Anmeldung zum **PSS.312 Cyber Resilience Act (CRA) für Hersteller von Maschinen und Geräten** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/trainings/pss-312/

PSS.321 Security Testing Foundation

2 Tage

Kosten/Teilnehmer: € 1.620,– zzgl. MwSt.
Mindestteilnehmeranzahl: 8 Personen

Tester

eigenes Notebook notwendig

Erfahrung in Web-Technolgien

Schulungsunterlagen und Teilnahmezertifikate

Inhouse / Inhouse Online

Security Testing Foundation

Das Security Testing Foundation Training lehrt die grundlegenden Konzepte des Security Testings. Es wird ein strukturiertes Vorgehen aufgezeigt und wie Security Tests für eine Applikation organisatorisch gestaltet werden können. Anschließend wird mit Fokus auf Web-Applikationen auf Cross-Site-Scripting- und SQL-Injection-Angriffe eingegangen und anhand von realen Beispielen ihre Anatomie erklärt und geübt. Während der Schulung wird immer wieder auf bekannte Hacking Tools zurückgegriffen, um den Teilnehmern ein reales Bild der Praxis zu vermitteln. Abschließend werden Tools vorgestellt, mit denen automatisierte Security Scans durchgeführt werden können und wie in weiterer Folge mit deren Ergebnissen umgegangen werden soll.

Das Training kann auch mit einem Fokus auf Security Testing für Embedded Devices abgehalten werden. Die Web-Themen werden dafür entsprechend durch relevanten Security Testing Themen aus Firmware, Hardware und Systemhärtung ersetzt als auch durch Inhalte für den Test von proprietären Protokollen und Interfaces erweitert.

Trainingsinhalte

Tag 1

Einführung
  - Guidelines und Standards
  - Threat Modeling
  - Definition von Scope und Testfällen
  - Vorbereitung der Testumgebung
Security Testing für Kryptographie
  - Verschlüsselung
  - Hashes
  - Digitale Signaturen
  - TLS
Security Testing für Web-Applikationen
  - OWASP Top 10 und OWASP ASVS
  - Testing mit Burp Suite
  - Weitere Tools zum Web-Applikation-Testing
Security Testing für mobile Applikationen
  - Exponierte Komponenten
  - Lokal gespeicherte Daten

Tag 2

Security Testing für Authentifizierung
  - Umgehung von Authentifizierungsschemas
  - Brute-forcing Angriffe
  - Directory Traversal Angriffe
  - Privilege Escalation
Security Testing von selbst entwickelten Schnittstellen und Protokollen
  - Fuzzing
  - Analyse und Testing Tools
Security Testing für System Härtung
  - System Härtung
  - Discovery Tools
  - Automatisierte Schwachstellen Scans
  - Konfigurationstests
Ergebnissammlung und -aufbereitung
  - Welche Information zählt?
  - Vulnerability Management

Das Training ist ideal geeignet für ...

Softwaretester und Softwareentwickler, die einen Einblick in die Grundlagen von Security Testing bekommen wollen.

Die Teilnehmer sollten nach der Ausbildung ...

verstehen, wie Angriffe funktionieren und beginnen wie ein Angreifer zu denken.
den Umgang mit automatisierten Testing-Tools beherrschen, um effizient wiederkehrende Testfälle abdecken zu können.
in der Lage sein identifierte Schwachstellen sinnvoll zu dokumentiert, um Nachvollziehbarkeit und Nachtests zu vereinfachen.

Anmeldung

Die Anmeldung zum **PSS.321 Security Testing Foundation Training** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/trainings/pss-321/

PSS.331 Sichere Embedded & (I)IoT-Produkte

3 Tage

Kosten/Teilnehmer: € 2.350,– zzgl. MwSt.
Mindestteilnehmeranzahl: 8 Personen

Entwicklungsleiter, Entwickler, Architekten, Tester, SecDevOps, CE-Beauftragte

eigenes Notebook notwendig

keine Vorkenntnisse notwendig

Schulungsunterlagen und Teilnahmezertifikate

Inhouse / Inhouse Online, Public / Public Online

Security in Embedded & (I)IoT-Produkten richtig und ganzheitlich umsetzen

Um Security in einem Produkt korrekt umzusetzen, ist ein ganzheitlicher Ansatz entscheidend. In diesem Training werden die notwendigen Bausteine für eine sichere Lösung besprochen und Möglichkeiten & Limitationen aufgezeigt. Von regulatorischen Anforderungen und Bedrohungsmodellierung über verschiedene Technologien, die für die Umsetzung relevant sein können (Virtualisierung, Secure Boot, Secure Storage,...) bis hin zu sicheren Entwicklungspraktiken und Testwerkzeugen wird den Teilnehmern im Training „Sichere Embedded & (I)IoT-Produkte“ vermittelt, wie Security in Produkten umgesetzt und verifiziert werden kann, so dass Produkte für ihre Einsatzumgebung ausreichend abgesichert sind.

Trainingsinhalte

Tag 1 (Anforderung)

- Regularien und Standards
  - Regularien (NIS, CRA, RED, MVO)
  - IEC 62443
- Security Fundamentals
- Security Management
  - Rollen, Verantwortlichkeiten und Expertise
  - Integritätsschutz (Code Signing)
  - Lieferantenmanagement (SBOM)
  - Vulnerability Monitoring (CVSS, CVE)
- Threat Modelling
  - Safety vs. Security
  - Threat Modelling Methodik

Tag 2 (Design)

- Secure by Design
  - Best Practices
  - Defense In Depth, Least privilege, Least functionality, Secure Patterns, Secure by Default,...
  - System Hardening (Linux, Windows, RTOS ...)
- Security Technologies
  - Security Components (TPM, Secure Element, SOC Features)
  - Chain of Trust (Secure Boot)
  - Secure Storage
  - Secure Interfaces und Update
  - Virtualisierung
  - Audit/Logging
  - Sichere Kommunikation und Protokolle

Tag 3 (Implementierung & Verifizierung)

- Sichere Implementierung
  - Coding Standards
  - Reviews
- Hardware Security
- Security Testing
  - Fuzzing
  - Code-Analyse-Tools
  - Binary Analysis

Das Training ist ideal geeignet für Hersteller von ...

- OT-Komponenten
- Maschinen
- IoT-Produkten
- Embedded Lösungen

Die Teilnehmer sollten nach der Ausbildung ...

- die Notwendigkeit von „Sicherer Produktentwicklung” verstehen
- die Grundlagen von Security verstehen und nachvollziehen können (u.a. Kryptographie, Secure Design Praktiken)
- relevante Security Komponenten/Bausteine für die System Architektur kennen und auswählen können (TPM, Secure Boot, Secure Storage,...)
- Test Werkzeuge kennen und im Entwicklungsprozess anwenden können

Anmeldung

Die Anmeldung zum **PSS.331 Sichere Embedded & (I)IoT-Produkte** finden Sie unter nebenstehendem Link oder durch Scannen des QR-Codes.

https://limessecurity.com/academy/trainings/pss-331/

Gültigkeit des Kursbuchs

Dieses Kursbuch gilt von 1. Juli 2026 bis 30. Juni 2027, bisherige Angebote verlieren damit ihre Gültigkeit.
Preise sind freibleibend und gelten bei Anmeldung bzw. Bestellung bis 30. Juni 2027.
Bei Abweichungen der Inhalte gelten die Informationen auf der Website.

www.limessecurity.com

Auszug Teilnahmebedingungen
Die vollständigen AGBs finden Sie unter
https://limessecurity.com/de/teilnahmebedingungen.

Die angeführten Kosten gelten in Euro exkl. USt und sind nach Rechnungserhalt innerhalb von 15 Tagen zu überweisen. Findet ein Training nicht statt, werden bereits hinsichtlich der Teilnahme geleisteten Zahlungen dem Teilnehmer ohne Abzüge erstattet. Umbuchungen bzw. Stornierungen müssen schriftlich erfolgen und sind bis 7 Werktage vor Veranstaltungsbeginn kostenfrei. Ab 6 bis 1 Werktagen vor Veranstaltungsbeginn werden für Umbuchungen 10 % bzw. für Stornierungen 30 % des Teilnahmebetrages verrechnet. Bei Nichterscheinen oder Stornierung ab dem (ersten) Tag der Veranstaltung wird der volle Teilnahmebetrag verrechnet, eine Umbuchung ist nicht mehr möglich. Gerne akzeptieren wir eine/n Ersatzteilnehmer/in.

Impressum
Herausgeber: Limes Security GmbH, Softwarepark 49
4232 Hagenberg, Tel: +43 720 510251
E-Mail: office@limessecurity.com
Firmenbuchnummer: 390566 m, Landesgericht Linz,
UID-Nummer: ATU 676 527 29;
Für den Inhalt verantwortlich: Limes Security GmbH,
Satz- und Druckfehler vorbehalten; v7.0_01_2025

https://limessecurity.com/de/teilnahmebedingungen

LIMES SECURITY