Zertifikatslehrgang

Security Intelligence Analyst, BdSI

Frühzeitige Identifizierung und Analyse von Unternehmensrisiken – Entwicklung geeigneter Gegenmaßnahmen

Lehrgangstermine 2025

Grundlehrgang: 11.-13.03.2025
Aufbaulehrgang: 06.-08.05.2025
in Bonn

Ausgebucht

SIMEDIA Akademie

Vorwort

In der heutigen dynamischen und vernetzten Geschäftswelt sehen sich Unternehmen mit immer häufigeren **komplexeren Bedrohungen und Herausforderungen** konfrontiert. Cyberangriffe, Wirtschaftsspionage, interne Sicherheitslücken, Rufschädigungen und geopolitische Instabilitäten sind nur einige der Risiken, die moderne Unternehmen bewältigen müssen.
Ein **effektives Sicherheits- und Risikomanagement** erfordert daher nicht nur reaktive Maßnahmen, sondern vor allem eine **proaktive und ganzheitliche Herangehensweise**.

Security Intelligence stellt einen umfassenden Ansatz dar, relevante und verwertbare Informationen für die Sicherheit eines Unternehmens zu erfassen und zentral auszuwerten.

Der **6-tägige Zertifikatslehrgang zum „Security Intelligence Analyst, BdSI"** bildet Fachkräfte weiter, die anschließend mit fundiertem Wissen und praktischen Fähigkeiten ausgestattet sind, um mit professionellen Methoden und Tools zu verwertbaren Informationen zu gelangen, um durch deren Analyse die Sicherheitsinteressen eines Unternehmens effektiv zu schützen und weiterzuentwickeln. Die Kombination aus theoretischen Grundlagen und praktischen Anwendungen stellt sicher, dass die Teilnehmer optimal auf ihre Rolle als Security Intelligence Analyst vorbereitet sind.

Der Zertifikatslehrgang besteht aus einem jeweils dreitägigen Grund- und Aufbaulehrgang.

Die Prüfung zum **„Security Intelligence Analyst, BdSI"** kann nur abgelegt werden, wenn beide Lehrgangsteile erfolgreich nacheinander abgeschlossen wurden. Eine Zulassung zu der Prüfung mit nur einem besuchten Lehrgangsteil ist ausgeschlossen.

Zielgruppe:
Sicherheitsmanager und Sicherheitsbeauftragte, Risikomanager, IT- und Cybersecurity-Experten, Compliance- und Datenschutzbeauftragte, Unternehmensberater und Wirtschaftsprüfer

Inhalte

Grundlagen der Intelligence-Arbeit
Die Teilnehmer erhalten eine Einführung in die wesentlichen Konzepte und Methoden der Intelligence-Arbeit. Es wird erklärt, warum Ressourcen in diesen Bereich investiert werden sollten und welche realistischen Ziele erreicht werden können. Die Teilnehmer lernen, wie man Informationen strukturiert sammelt, analysiert und interpretiert, um fundierte Entscheidungen treffen zu können. Außerdem werden die verschiedenen Zielgruppen und Empfänger von Intelligence-Produkten behandelt sowie die Bedeutung der Prognostizierbarkeit und der Früherkennung von Trends.

Open-Source Intelligence (OSINT)
Der Fokus liegt auf den Grundlagen und Anwendungen der Open Source Intelligence. Die Teilnehmer lernen, was OSINT und Social Media Intelligence (SocMint) sind und wie sie genutzt werden können. Es werden verschiedene Informationsquellen vorgestellt, einschließlich sozialer Netzwerke und anderer offener Quellen. Die Teilnehmer üben die Anwendung von Techniken und Methoden des OSINT, um relevante Informationen zu extrahieren, zu analysieren und für die Sicherheitsinteressen ihres Unternehmens zu nutzen. Praktische Übungen mit kostenlosen und kommerziellen OSINT-Tools runden dieses Modul ab.

Anwendungsfälle und Methoden
Spezifische Anwendungsfälle von OSINT in der Unternehmenssicherheit werden behandelt. Die Teilnehmer erfahren, wie OSINT zur Bedrohungsanalyse, Rufschädigungserkennung und Identifizierung von Sicherheitslücken eingesetzt werden kann. Es werden methodische Ansätze wie der Risikokatalog, die Informationskette und der Intelligence Cycle vorgestellt. Die Teilnehmer erlernen, wie sie aus gesammelten Daten verlässliche Informationen und Erkenntnisse gewinnen und diese in praktische Handlungsempfehlungen umsetzen können.

Rechtliche Rahmenbedingungen und ethische Aspekte
Die rechtlichen und ethischen Aspekte der Intelligence-Arbeit werden behandelt. Es wird ein umfassender Überblick über die Datenschutzgrundverordnung (DSGVO) und ihre Relevanz für OSINT-Aktivitäten gegeben. Darüber hinaus wird der EU-KI-Act und seine Auswirkungen auf die Nutzung von künstlicher Intelligenz in der Intelligence-Arbeit behandelt. Die Teilnehmer lernen, wie sie sicherstellen können, dass ihre Methoden und Praktiken den gesetzlichen Vorgaben entsprechen und ethische Standards einhalten. Dies schützt das Unternehmen vor rechtlichen Konsequenzen und wahrt das Vertrauen der Öffentlichkeit.

Tag 1:

Grundlagen und Zielsetzung der Intelligence-Arbeit

(Grundlehrgang: Grundlagen der Intelligence-Arbeit und Unternehmenssicherheit)

11. März 2025
Beginn: 9:00 Uhr

Zielsetzung / Zweck Intelligence

- Einführung in die Relevanz und Notwendigkeit von Intelligence-Arbeit
- Zielgruppen und Empfänger von Intelligence-Produkten
- Was ist Intelligence?

Grundüberlegungen zur Intelligence-Arbeit

- Prognostizierbarkeit und Früherkennung von Trends
- Sicherheitsinteressen und Relevanz für das Unternehmen
- Anwendungsfälle im Unternehmen
- Zuverlässigkeit von Informationen und Eintrittswahrscheinlichkeiten (Quell- und Informationssicherheit – 4x4 / 6x6)

Methodischer Ansatz I – Risikokatalog

- Teamarbeit zur Erstellung eines Risikokatalogs
- Diskussion und Erstellung eines Best Practice-Katalogs

Methodischer Ansatz II – Bias und Heuristiken

- Welchen Grundannahmen sitzen wir auf?
- Konzepte zu Kognitive Verzerrungen (Biases und Heuristiken)

Ende: 17:00 Uhr

Tag 2:

Informationsquellen und Methoden der Intelligence-Arbeit

12. März 2025
Beginn: 9:00 Uhr

Informationsquellen – intern und extern

- Unternehmensinterne und -externe sicherheitsrelevante Informationen
- Bewertung der Zuverlässigkeit und Nutzung von Informationen

Methodischer Ansatz II – Informationskette

- Von Daten über Informationen zu Wissen und Handeln

Methodischer Ansatz III – Intelligence Cycle

- Ziel / Aufgabe, Sammeln / Recherchieren, Bewerten, Verknüpfen, Analyse / Hypothesen, Report

Methodischer Ansatz IV – Szenarienbildung & Prognosen

- Bewährte Methoden der Szenarienbildung
- Anwendung in Sicherheitsbehörden, Nachrichtendiensten und Militär

Ende: 17:00 Uhr

Tag 3:

Bewertung, Empfehlungen und rechtliche Rahmen-bedingungen

13. März 2025
Beginn: 9:00 Uhr

Methodischer Ansatz V – Analyse Methodiken I – Organisationsmethodiken

- Teilnehmererfahrungen und Best Practices

Methodischer Ansatz VI – Analyse Methodiken II

- Darstellung und Anwendung Explorativer, Diagnostischer Analysetechniken
- Reframing und Foresight Techniken im Einsatz

Methodischer Ansatz VII – Decision Support

- Wie komme ich zur Entscheidung
- Darstellungs- und Präsentationsmöglichkeiten

Ausblick – PPP in Deutschland

- Aktivitäten der Allianz für Sicherheit in der Wirtschaft
- Initiative für Wirtschaftsschutz

Abschluss – Zusammenfassung und Erkenntnisse

- Zusammenfassung und Diskussion der Erkenntnisse
- Ergänzungs- und Vertiefungsbedarf

Ende: 17:00 Uhr

Tag 4:

Grundlagen und Einführung in OSINT

(Aufbaulehrgang: Teil 2: Vertiefung in Intelligence-Arbeit und OSINT.)

06. Mai 2025
Beginn: 9:00 Uhr

Strukturierte Analyse

- Strukturierte Analyse – Intelligence Cycle, Quell- und Informationssicherheit Vertiefung

Grundlagen von OSINT

- Definition und Bedeutung von OSINT und Social Media Intelligence (SocMint)
- Überblick über verfügbare Quellen und deren Relevanz

Informationsquellen und Techniken

- Soziale Netzwerke, Foren und andere offene Informationsquellen
- Techniken zur Informationsbeschaffung und -auswertung
- Quellbewertungen

Ende: 17:00 Uhr

Tag 5:

Praktische Anwendung von OSINT-Methoden

07. Mai 2025
Beginn: 9:00 Uhr

Anwendungsfälle für Unternehmenssicherheit

- Bedrohungsanalyse, Rufschädigungserkennung und Identifizierung von Sicherheitslücken
- Praktische Beispiele und Fallstudien

Methoden und Techniken der OSINT

- Vertiefung in spezifische OSINT-Techniken
- Praktische Übungen und Workshops

Toolgestützte OSINT

- Vorstellung und Anwendung kostenfreier und kommerzieller OSINT-Tools
- Praktische Übungen zur Nutzung der Tools
- Abgrenzung der Einsatzszenarien
- Protokollierung und Sicherung

Ende: 17:00 Uhr

Tag 6:

Toolgestützte OSINT und rechtliche Rahmenbedingungen

08. Mai 2025
Beginn: 9:00 Uhr

Toolgestützte OSINT

- Vorstellung und Anwendung kostenfreier und kommerzieller OSINT-Tools
- Praktische Übungen zur Nutzung der Tools

Rechtliche Rahmenbedingungen und ethische Aspekte

- Datenschutz-Grundverordnung (DSGVO) und EU-KI-Act
- Ethische Standards und Rechtliche in der Intelligence-Arbeit

Abschluss und Zertifizierung

- Zusammenfassung der Lehrgangsinhalte
- Diskussion der Erkenntnisse und Abschlussprüfungen
- Übergabe der Zertifikate

Ende: 17:00 Uhr

Referenten

Schwerdtner, Robert
Leiter des Bereichs Solution Design bei der Rola Security Solutions GmbH. Er verfügt über umfangreiche praktische Erfahrung als Analyst und Projektverantwortlicher bei großen deutschen Sicherheitsbehörden. In seiner aktuellen Position ist er verantwortlich für die Entwicklung innovativer Lösungen und Methoden im Bereich der sicherheitsbehördlichen Analyse. Zuvor leitete er den Aufbau der SocMint-Analysefähigkeiten im Konzernlagezentrum der Deutschen Telekom AG.

Weis, Nico
Teamleiter des Deeskalationsmanagements für das Lösungsgeschäft für Individual & Großkunden der Deutschen Telekom AG. Weiterbildungen in den Bereichen Social Media Marketing, Social Media Unternehmensportfolios, Datenschutz und Projektmanagement. Referent zum Thema Social Media Gefahren, Nutzung und Chancen.

Anmeldebedingungen

Veranstaltungsort

Dorint Hotel Bonn, Berliner Freiheit 2, 53111 Bonn, Tel: +49 228 72690, E-Mail: info.bonn@dorint.com. Es steht ein begrenztes Zimmerkontingent **bis 4 Wochen** vor Veranstaltungsbeginn zur Verfügung. Bitte nehmen Sie die Reservierung unter Berufung auf Ihre Teilnahme an der Veranstaltung selbst vor.

Kosten

Die Teilnahmegebühr für den zweitägigen Grundlehrgang beträgt € 2.250,–, für den viertägigen Aufbaulehrgang € 4.500,– und ist nach Rechnungserhalt vor Beginn der Veranstaltung zu entrichten. Der Preis versteht sich zuzüglich Mehrwertsteuer. Darin enthalten sind eine digitale Dokumentation, Mittagessen, Erfrischungen und Pausenverpflegung sowie das gemeinsame Abendessen zwischen zwei gebuchten Veranstaltungstagen.

Anmeldung

Ihre Anmeldung und Zahlung richten Sie bitte an die SIMEDIA Akademie GmbH, Alte Heerstraße 1, 53121 Bonn. Nach Eingang Ihrer Anmeldung, die Sie telefonisch +49 228 9629370, per E-Mail anmeldung@simedia.de oder über das Internet unter www.simedia.de vornehmen können, erhalten Sie die Anmeldebestätigung und detaillierte Informationen zur gebuchten Veranstaltung sowie das Hotel. Die SIMEDIA Akademie behält sich vor, Anmeldungen ohne Angabe von Gründen abzulehnen.

Stornierung / Rücktritt

Wenn Sie bereits verbindlich zu einer Veranstaltung angemeldet sind, aber nicht teilnehmen können, stehen Ihnen folgende Möglichkeiten zur Verfügung:
Bis unmittelbar vor Beginn einer Veranstaltung können Sie einen Kollegen (Ersatzperson) benennen. Dafür entstehen Ihnen keine weiteren Kosten.
Bis 4 Wochen vor der Veranstaltung können Sie die Teilnahme kostenlos stornieren. Der Rücktritt muss immer schriftlich (per E-Mail) erfolgen.

- Erfolgt der Rücktritt zwischen 30 und 8 Tagen vor Veranstaltungsbeginn, werden wir 50% der Teilnahmegebühr berechnen.
- Erfolgt der Rücktritt nach weniger als 8 Tagen vor der Veranstaltung, ist die volle Teilnahmegebühr zu entrichten.

Erscheint der Teilnehmer nicht, ohne abgesagt zu haben, sind wir berechtigt, die volle Veranstaltungsgebühr in Rechnung zu stellen. Sollte die Veranstaltung seitens SIMEDIA Akademie GmbH abgesagt werden, so besteht ein Anspruch auf volle Rückerstattung der Teilnahmegebühr; Ansprüche darüber hinaus bestehen nicht.