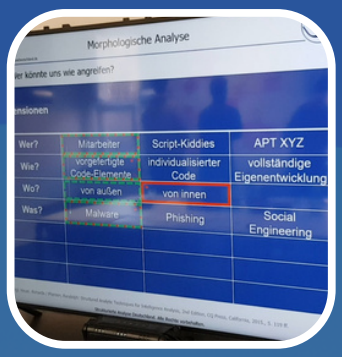
Strukturierte Analyse Deutschland

KOMPAKT-TRAINING ANALYTIC TRADECRAFT FOR CYBER THREAT INTELLIGENCE

HAMBURG - 15.09.2026 - 16.09.2026



Lernziele auf einen Blick:

- Was ist Intelligence und was ist vor diesem Hintergrund CTI?
- Kognitionspsychologische Grundlagen der Analyse
- Die Rolle von Fragestellungen für die Analyse
- Bedeutung adressatengerechter Produkte
- Anwendung Strukturierter Analysetechniken (SATs) in realistischen CTI-bezogenen Szenarios:
  Analytisches Spektrum, Issue Redefinition, Customer Checklist, Getting Started Checklist, Morphologische Analyse, Cluster Brainstorming, Simple Hypothesis, Multiple Hypothesis Generator, Analysis of Competing Hypotheses, AIMS

KOMPAKT-TRAINING ANALYTIC TRADECRAFT FOR CYBER THREAT INTELLIGENCE

TRAININGSABLAUF

Intelligence und CTI

Auffrischung: Was ist Intelligence und der Intelligence Cycle und wie fügt sich Cyber Threat Intelligence in diese Konzepte ein?

Psychologie der Analyse

Analyse findet nicht im luftleeren Raum statt. Sowohl der Prozess der Analyse als auch Analyseergebnisse werden von diversen kognitionspsychologischen Faktoren beeinflusst. Diese zu kennen ist eine Voraussetzung für reflektierte Intelligence Prozesse und Produkte.

Rolle von Fragen

Fragen spielen eine entscheidende Rolle für Intelligence Prozesse und Produkte. Allerdings wird dem Thema oft nur wenig Raum gegeben. In diesem Abschnitt gewinnen Sie einen Überblick über die wichtigsten Eckdaten und lernen, worauf Sie achten müssen.

Fragenraum organisieren

Nur wenn Sie einen Überblick über den für Sie relevanten Fragenraum gewonnen haben, können Sie entscheiden, welche Fragen wirklich wichtig sind und beantwortet werden sollten. In diesem Abschnitt lernen Sie wie Sie diese Herausforderung meistern.

Know your Audience

Intelligence Produkte müssen Relevanz entfalten, wenn sie wirken sollen. Dazu ist es notwendig, die Adressatin oder den Adressaten zu kennen. In diesem Abschnitt lernen Sie zwei SATs kennen, mit denen dieser Schritt erleichtert wird.

Struktur und Kreativität

Feindselige Akteure sind stets darauf bedacht neue Wege zu finden, um (digitale) Schutzgüter von Unternehmen und staatlichen Organisationen anzugreifen. In diesem Abschnitt lernen Sie, wie Sie der Kreativität des Angreifers mit eigener Kreativität und Struktur begegnen können.

Arbeit mit Hypothesen

Um unklare Geschehnisse oder Aktivitäten einordnen und erklären zu können, ist die Arbeit mit Hypothesen oft unvermeidbar. In diesem Abschnitt erlernen Sie, wie Sie strukturiert Hypothesen generieren und testen.

Ihr Dozent für dieses Training: Ole Donner
Gründer des Trainings- und Beratungsunternehmens „Strukturierte Analyse Deutschland“

KOMPAKT-TRAINING ANALYTIC TRADECRAFT FOR CYBER THREAT INTELLIGENCE

AUF EINEN BLICK

In diesem Training befähigen wir die Teilnehmenden Problemstellungen der Cybersicherheit strukturiert zu begegnen. Der Schwerpunkt des Trainings liegt daher in der praktischen Vermittlung und Anwendung unterschiedlicher Analysetechniken entlang realistischer Beispiele. Damit führt dieses Training zwei wesentliche Bereiche zusammen: Intelligence und Cybersicherheit.

Im Schwerpunkt richtet sich dieses Training an Senior Analysts aus dem defensiven Bereich der Cybersicherheit („Blue-Teamler", CISOS, SOC Manager, CTI Manager, Forensic Manager, Collection Manager sowie Personal aus CDOCs, SOCs etc.). Teile des Trainings sind darüber hinaus gewinnbringend für Personal aus dem offensiven Bereich (Pen-Tester, „Red-Teamler" etc.).

Design Offices Hamburg
Hammerbrook
Sachsenstraße 20
20097 Hamburg

Tag 1:
- Intelligence und CTI
- Grundlagen der Analyse
- Die Rolle von Fragestellungen verstehen

Tag 2:
- Checklisten
- Kreativitätstechniken
- Hypothesen generieren und testen

15.09.2026
10:00 Uhr bis 18:00 Uhr

16.09.2026
09:00 Uhr bis 17:00 Uhr

Für das leibliche Wohl während des Trainings ist gesorgt.

1.750 € inkl. Mwst.

Teilnahmezertifikat

Testimonials

"In a world where technology advancements are only outpaced by the growth of the attack surface we are trying to defend, the use of the intelligence cycle and its associated techniques is of primordial importance to safeguard both the public and private sector in the virtual world."*

*Source: Dion, Martin: Intelligence and Cyber Threat Management – Appyling Foresight and Analytical Techniques to Mitigate Cyber Risks, in: Bartsch, Michael / Frey, Stefanie (Hrsg.): Cybersecurity Best Practices – Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, Springer: 2018, (p. 363-392) p. 363.

Sehr zu empfehlender Kurs mit guten Praktiken, die in der Praxis umgesetzt werden können.

– R. RAMADANOSK, SOC ANALYST

Ein sehr empfehlenswertes, anschauliches Training. Ole Donner schafft es, komplexe Analysemethoden gut zu erklären und man hatte trotz der Anstrengung Spaß.

– L. WOTH – PENETRATION TESTER

Die hier verwendeten Fotos bilden nicht die real bewertenden Personen ab.