Fraunhofer
ACADEMY

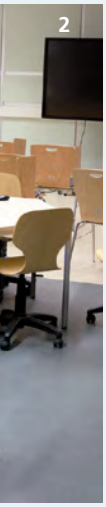
Weiterbildung im
Lernlabor Cybersicherheit

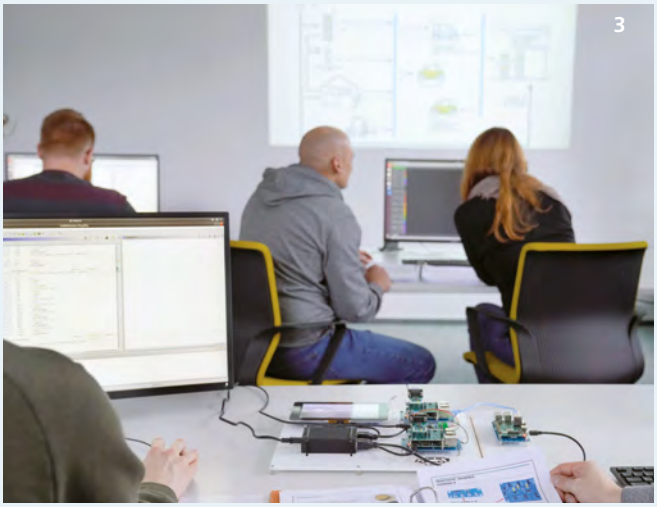
Know-how für mehr IT-Sicherheit

IT-Forensik

www.cybersicherheit.fraunhofer.de

Inhalt





Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy im Bereich Information und Kommunikation. Im Zentrum des umfassenden Angebots des Lernlabors stehen alle Themen rund um die IT-Sicherheit.

Impressionen aus unseren Lernlaboren Cybersicherheit:

1 Lernlabor Cybersicherheit in Sankt Augustin: Techniken und Strategien für den Hochsicherheitsbereich kennenlernen, z.B. sichere biometrische Gesichts-erkennung.

2 Lernlabor für Cybersicherheit an der Hochschule Mittweida.

3 Das Lernlabor Cybersicherheit beim Fraunhofer SIT.

4 Eröffnung des Lernlabors Internetsicherheit und IT-Forensik am Standort Mittweida.

Mehr Sicherheit mit unseren Weiterbildungen

5 Gründe für die Weiterbildung im Lernlabor Cybersicherheit

5

Anerkannte Expertinnen und Experten

Profitieren Sie vom langjährigen Spezialwissen unserer Expertinnen und Experten aus der Forschung und unseren Entwicklungs- und Beratungsprojekten. In Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen erhalten Sie verwertbare, neueste Erkenntnisse auf allen Gebieten der Cybersicherheit.

Bei uns bekommen Sie Wissen aus erster Hand

Unsere Kurse sind nicht nur auf dem aktuellsten Stand der Forschung, sie orientieren sich auch passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Im Team trainieren und erarbeiten Sie Lösungskonzepte in den Bereichen, die für Sie tatsächlich relevant sind.

Maßgeschneiderte Inhouse-Seminare

Integrieren Sie die Weiterbildung zum Thema Cybersicherheit direkt in Ihr Unternehmen, für mehrere Mitarbeitende oder Abteilungen. Dafür passen wir die Inhalte individuell auf Ihre Bedarfe an. Wir beraten Sie gerne, welche Lösung für Sie die optimale darstellt.

Für jede Situation das passende Seminar

Ein Universalkonzept bei IT-Sicherheitslösungen gibt es nicht! Die Komplexität und das Spektrum an Problemfeldern ist einfach zu groß. In unserem breiten Themenangebot finden Sie jedoch garantiert die passende Weiterbildung. Zugeschnitten auf Ihren Kenntnisstand und auf Ihr Spezialgebiet. Ob als Onlineseminar, Präsenzseminar oder Mix aus beidem.

Lernlabore

An zahlreichen Standorten in Deutschland können Sie in unseren modernen Lernlaboren mithilfe hochwertiger technischer Infrastruktur reale Bedrohungsszenarien nachstellen und durchspielen. Anhand konkreter Anwendungsfälle wird so das Gelernte für Sie erfahrbar und direkt umsetzbar.

Kompetenzaufbau auf allen Ebenen

IT-Sicherheitswissen betrifft nicht mehr nur Spezialistinnen und Spezialisten, auch entscheidungsbefugte Personen, Fachkräfte und Anwendende sollten lernen, Sicherheitsrisiken abzuschätzen und diese zu beherrschen. Hierfür benötigen die Mitarbeitenden eine Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und die Konsequenzen von IT-Sicherheitsproblemen in ihrem Verantwortungsbereich. Das Lernlabor richtet sich deshalb an folgende Zielgruppen mit jeweils spezifischen Seminaren:

Führungskräfte, die Entscheidungsprozesse verantworten müssen, benötigen einen verständlichen Überblick über aktuelle Gefahren, Sicherheitsstrategien und Methoden.

Sicherheitsexpertinnen und -experten mit einer IT-Sicherheits-ausbildung oder entsprechender Berufserfahrung können ihr Wissen auf den neuesten Stand bringen.

Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

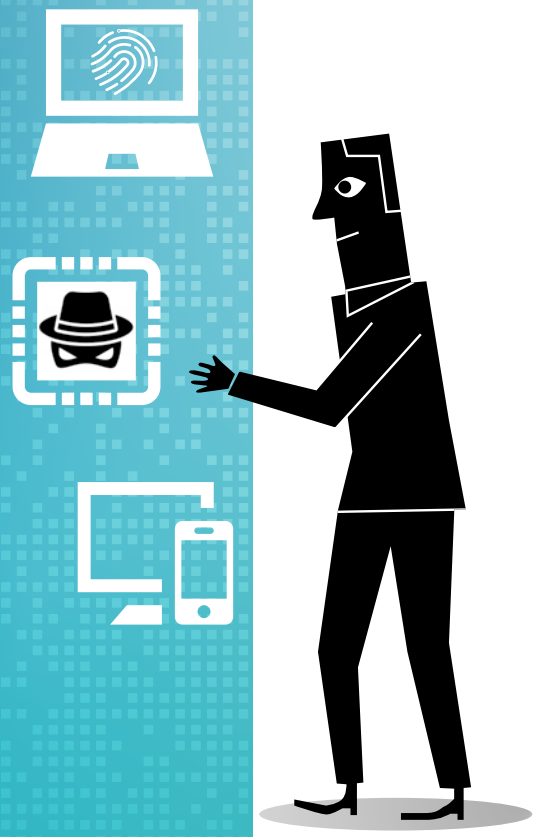
IT-Nutzerinnen und -Nutzer ohne spezifische Fachkenntnisse, von denen erwartet wird, dass sie Sicherheitsbewusstsein aufbauen und sicherheitskonformes Verhalten entwickeln.

Erklärung der Symbole auf den Seminarseiten

- Abschluss
- Voraussetzungen
- Zielgruppe
- Dauer
- Kosten
- Örtlichkeit

IT-Forensik

Digitale Spuren sammeln und analysieren



Die Aufgabe der digitalen Forensik ist die Sicherung und Auswertung von digitalen Beweisen, etwa um Straftaten aufzuklären, Sicherheitslücken zu schließen oder Authentizität von Daten zu prüfen. Denn Cybercrime, Fake News, Wirtschaftsspionage, unbeabsichtigte Datenlecks, Betrugsvorfälle und die digitale Informationsflut allgemein sind große Herausforderungen. Doch welche Werkzeuge sind in welchem Fall geeignet? Wie sieht eine fundierte IT-forensische Datenanalyse aus? Wesentlich für den Erfolg ist ein methodisches Vorgehen, das spezielle Expertise benötigt.

Der Austausch von digitalen Daten steigert das Manipulationspotenzial und öffnet Schwachstellen. Auch im Privaten wächst die Nutzung digitaler Technologien. Gerade im Bereich der Strafverfolgung gewinnen digitale Daten daher immer mehr an Relevanz.

Ein strukturiertes, methodisches Vorgehen in der IT-Forensik ist daher besonders entscheidend für den Erfolg der Aufklärung. Nur mit einer verlässlichen Beweiskette kann der Ursprung und die verantwortliche Person ausfindig gemacht werden.

Im Lernlabor Cybersicherheit lernen Sie das aktuelle Spektrum der Werkzeuge für IT-Forensik und OSINT-Recherche im Internet kennen. Auf Basis wissenschaftlicher Erkenntnisse werden Sie in unseren Seminaren mit den aktuellen Trends vertraut gemacht und können so Ihr Wissen erweitern.

Digitale Forensik und OSINT können Ihnen helfen, Sicherheitsvorfälle aufzuklären, »gelöschte« Daten wiederherzustellen, Manipulationen Ihrer Beweismittel zu erkennen, und gezielt zu Ihren Security-Herausforderungen online zu recherchieren.


OSINT
GUTACHTEN
METADATEN
TEXTDATEN
DATENSICHERUNG
DATENQUELLEN
DATENREKONSTRUKTION
IT-FORENSIK
DATEN
ANALYSE
MACHINE
LEARNING
SPURENSUCHE
ECHTHEITSPRÜFUNG
MANIPULATION
METHODIK
WERKZEUGE
VERSCHLÜSSELUNG
CYBERANGRIFFE
TEXTANALYSE
MULTIMEDIADATEN

Informationen im Überblick

Allgemeine IT-Kenntnisse

Fach- und Führungskräfte in Unternehmen und Behörden für Ermittlung, IT-Sicherheit, IT-Betrieb oder Compliance

8 Stunden an 3 Tagen

600,–

online

Dieses Seminar eignet sich auch besonders als vertrauliche Inhouse-Schulung. Fragen Sie uns an: **cybersicherheit@fraunhofer.de**

Veranstaltet durch

Fraunhofer SIT

Referenten:

York Yannikos,
stv. Abteilungsleitung,
Mediensicherheit
und IT-Forensik,
Fraunhofer SIT

Dr. Sascha Zmudzinski,
wiss. Mitarbeiter
Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/grundl-datentraegerforensik

Einführung in die Datenträgerforensik

Einsatzmöglichkeiten für IT-Forensik verstehen

Die Aufklärung von IT-Sicherheitsvorfällen gehört in Unternehmen zu den Aufgaben von Beauftragten für IT-Sicherheit, IT-Betrieb oder Compliance. Oftmals befinden sich hierzu Beweise auf Datenträgern in Arbeitsplatz-PCs oder Servern. In diesem Seminar erhalten Sie einen Überblick über geeignete Methoden der IT-Forensik für Datenträger.

Erstellung eines gerichtsverwertbaren Gutachtens

Übersicht Softwarewerkzeuge

PC-Demos mit »photorec« und »Autopsy/Sleuth Kit«

Inhalte des Seminars

Grundlagen
- Definition IT-Forensik
- IT-forensische Vorgehensweise: von der Vorbereitung bis zum Abschlussbericht

Datenträgerforensik
- Beweissicheres Anfertigen eines Datenträgerabbilds
- Datei- und Betriebssysteme
- Wiederherstellen »gelöschter« Dateien
- Forensische Analysemethoden

Ihr Nutzen

- Nach dem Seminar können Sie Forensikmethoden verstehen und auswählen.
- Sie sind in der Lage, einfache Untersuchungen von Festplatten, SSDs selbst durchzuführen.
- Sie können bei anspruchsvollen Untersuchungen externe forensische Gutachten beauftragen.

Car Forensik – Auswertung vernetzter Systeme

Kommunikation in der Kfz-Elektronik

In diesem Workshop lassen sich Theorie und Praxis miteinander vereinen. Lernen Sie welche Daten in welchen Steuergeräten abgelegt sind und wie diese ausgelesen werden können. Dabei steht das „Controller Area Network" als Bussystem im Mittelpunkt. Darüber hinaus werden auch Kfz-Schlüssel und deren Transponder untersucht. Im Verlauf des Seminars werden Varianten zur Manipulation von Wegstreckenzählern aufgezeigt und ein Ausblick auf die Funktionsweise von Car2X-Systemen sowie deren Manipulationsmöglichkeiten gegeben.

Inhalte des Seminars

Tag 1
- Einführung in die Car Forensik
- Kfz-Bussysteme
- Elektronische Wegfahrsperren
- Transponder
- Techniken
- KeylessGo
- Wegstreckenzähler
- Automotive Ethernet
- Car2X

Tag 2
- Car-Simulation mittels Linux (virtueller CAN-Bus)
- Steuerung der CAR-Simulation mit OLIMEX AT90CAN-Board über realen CAN-Bus
- Simulationsübung zum CAN-Bus mit CANoe
- CAN-Demonstrator mit CANoe programmieren
- LIN-Bus Simulation in CANoe

Tag 3
- Auslesen von Steuergeräten
- Reverse Engineering
- Vorführung: Analyse von Kfz-Schlüsseln per Tango-Programmer
- Auswertung

Ihr Nutzen

- Nach dem Workshop können Sie Steuergeräte über CAN-Bus auslesen.
- Sie können Daten in Fahrzeugen für Ihre forensische Arbeit nutzen.
- Sie werden die Funktionsweise von Wegfahrsperren verstehen.

Informationen im Überblick

Problemloser Umgang mit dem PC sowie IT-Grundkenntnisse

Versicherer, Gutachter*innen, Ermittler*innen, Jurist*innen

2,5 Tage Präsenz

1500,–

Mittweida

Dieses Seminar eignet sich auch besonders als vertrauliche Inhouse-Schulung. Fragen Sie uns an: **cybersicherheit@fraunhofer.de**

Veranstaltet durch

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Referent:

Dipl.-Ing. Heiko Polster, seit 2003 Entwicklungsingenieur an der Hochschule Mittweida

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/car-forensik

Informationen im Überblick

- Forensikgrundkenntnisse, Arbeiten auf der Kommandozeile (Windows, Linux)
- Forensiker*innen und Ermittelnde
- 15 Stunden an 4 Tagen
- 1200,–
- online

Veranstaltet durch

Fraunhofer SIT

Referenten:

York Yannikos, stv. Abteilungsleitung Mediensicherheit und IT-Forensik, Fraunhofer SIT

Lukas Graner, wiss. Mitarbeiter, Fraunhofer SIT

Dr. Sascha Zmudzinski, wiss. Mitarbeiter, Fraunhofer SIT

Prof. Martin Steinebach, Abteilungsleitung Mediensicherheit und IT-Forensik, Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/multimediaforensik

Multimediaforensik (Bild, Video und Audio)

Multimediadaten rekonstruieren und analysieren

Die Herausforderung: Wenn man Multimediadaten forensisch untersucht, müssen diese als »gelöschte« Dateien oftmals zuerst wiederhergestellt werden. Anschließend muss dann unter Umständen eine sehr große Anzahl von Dateien gesichtet werden. Dann erst können im Bild oder gegebenenfalls der Tonspur Spuren gesucht und gesichert werden. In diesem Seminar lernen Sie hierzu Prinzipen und moderne Methoden der Multimediaforensik für jeden dieser Arbeitsschritte kennen.

Inhalte des Seminars

Grundlagen: Basiswissen zu JPEG, Vorgehensmodell in der IT-Forensik

Datensammlung aus Endgeräten für Multimediadaten

Datenwiederherstellung, Datenuntersuchung

Automatische Verfahren zur Vorsortierung
- Robustes Hashing und Image Matching
- Deep Learning zur Medienklassifizierung

Untersuchung unsichtbarer/unhörbarer Informationen
- Metadatenanalyse
- Sensorfingerprinting (PRNU)
- ENF-Forensik
- Steganographie

Livedemos zu Filecarving, Metadaten, Hashes, »Kameraballistik«

Beweiskraft forensischer Spuren

Softwarewerkzeuge für Multimediaforensik

Praxistipps zur Dokumentation und Gutachtenerstellung

Ihr Nutzen

- Nach dem Seminar verstehen Sie die häufig eingesetzten Multimediadatenformate.
- Sie lernen Verfahren zum Rekonstruieren »gelöschter« Multimedia-Dateien kennen.
- Sie kennen Verfahren zum Sichten sehr großer Bilddatenmengen und können Metadaten in gängigen Medienformaten erfassen.
- Sie lernen Methoden kennen, mit denen Sie die Datenquelle identifizieren können (z.B. Kamera, Aufnahmegerät).
- Sie verstehen das Prinzip beim Einbetten versteckter steganographischer Botschaften in Bilddaten.

Manipulierte Digitalfotos und -videos erkennen

Manipuliertes Bildmaterial erkennen

Manipulierte Digitalfotos oder -videos können in Ermittlungsverfahren falsche Spuren legen. Und sie können als »Fake News« die öffentliche Meinung manipulieren. Denn Bildmaterial kann per Bearbeitungssoftware leicht verfälscht werden. Und es kann auch in die Irre führen, wenn man es unverändert, aber in einem anderen Kontext verwendet. Wir bieten Ihnen hierzu zwei Seminare unterschiedlicher Dauer und fachlicher Tiefe zu Methoden der Echtheitsprüfung bzw. dem Fact Checking von Bildmaterial.

Inhalte der Seminare

Modul »Forensische Echtheitsprüfung für Bild-/Videodaten«

- Technische Grundlagen
  - Basiswissen zu JPEG
  - Integrität und Authentizität
- Signalforensik unsichtbarer Spuren
  - Eigenschaften authentischer Daten
  - Einfluss durch Nachbearbeitung
- Metadatenuntersuchung
- Abgleich mit externen Referenzdaten
- Szenenbasierte Bildforensik
- Aktive Verfahren zur Echtheitsprüfung
- Beweiskraft forensischer Spuren
- Marktüberblick zu Softwarewerkzeugen
- PC-Übungen zum Erkennen von Bildmanipulationen, Metadatenuntersuchung

Modul »Faktenprüfung für Bildmaterial in 4 Stunden«

- Grundlagen: u.a. Arten der Desinformation
- Überblick modellbasierte Bildforensik
- Überblick Metadatenanalyse
- Überblick KI-basierte Bildforensik
- Inverse Bildersuche
- Demos / Fallbeispiele
- Softwarewerkzeuge + Literatur

Ihr Nutzen

- Sie können Dateiformate und den »Lebenszyklus« von Bildmaterial verstehen.
- Sie sind dazu in der Lage, Methoden mit denen Sie die Echtheit digitaler Bilder prüfen, zu verstehen und einzusetzen.

Informationen im Überblick

Allgemeine IT-Kenntnisse

IT-Forensiker*innen, Ermittelnde, Journalist*innen, Schadensregulierende, technikaffine Interessierte aus allen Fachrichtungen

Modul »Forensische Echtheitsprüfung für Bild-/Videodaten«

14 Stunden an 4 Tagen

1200,–

www.cybersicherheit.fraunhofer.de/pruefung-bild-videodaten

Modul »Faktenprüfung für Bild-/Videodaten in 4 Stunden«

4 Stunden

240,–

www.cybersicherheit.fraunhofer.de/faktenpruefung-bildmaterial

Referenten:

Dr. Huajian Liu und Dr. Sascha Zmudzinski, wiss. Mitarbeiter, Mediensicherheit und IT-Forensik, Fraunhofer SIT

Veranstaltet durch

Fraunhofer SIT

Informationen im Überblick

Gute Kenntnisse der Python-Programmierung

Forensiker*innen, Ermittler*innen, Data Scientists/Analysts, IT-Sicherheitsexpert*innen, Data Journalists, Social Media Manager, PR-Beratung, Financial Analysts

4 Tage

1500,–

online

Veranstaltet durch

Fraunhofer SIT

Referent*innen:

Lukas Graner,
wiss. Mitarbeiter,
Mediensicherheit
und IT-Forensik,
Fraunhofer SIT

Jeong-Eun Choi,
wiss. Mitarbeiterin,
Fraunhofer SIT

Inna Vogel,
wiss. Mitarbeiterin,
Mediensicherheit
und IT-Forensik,
Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/textanalyse

Textdatenanalyse mit NLP und Maschinellem Lernen

»Schürfen« in Textdaten (Einführungskurs)

Die Herausforderung: Ein Großteil der weltweit verfügbaren Informationen liegt in Texten vor. Für viele Anwendungen ist die Suche nach relevanten Informationen in Textdaten wichtig, z.B. um nach Themen, Schreibstilen oder Sentiment zu klassifizieren oder den Verfasser eines Textes zu identifizieren. Unser Einführungskurs bietet Ihnen hierzu wichtige Vorkenntnisse des Natural Language Processing (NLP) und des maschinellen Lernens (ML) vermittelt, in der Theorie und als »Python«-Quellcode.

Inhalte des Seminars

Crawling von WWW-Seiten

Korpuserstellung

Datenbereinigung und Preprocessing

Grundlagen des ML

Interpretierbarkeit von ML-Modellen

Statistische Evaluierung Ihrer Ergebnisse Überblick über Anwendungen: Autorschaftsanalyse, Topic Modeling, Sentiment-Analyse, Landessprachen-Erkennung

Livedemos zu den Kursthemen

Python-Programmierübungen als Jupyter-Notebooks

Intensive Online-Betreuung durch unsere Expertinnen und Experten

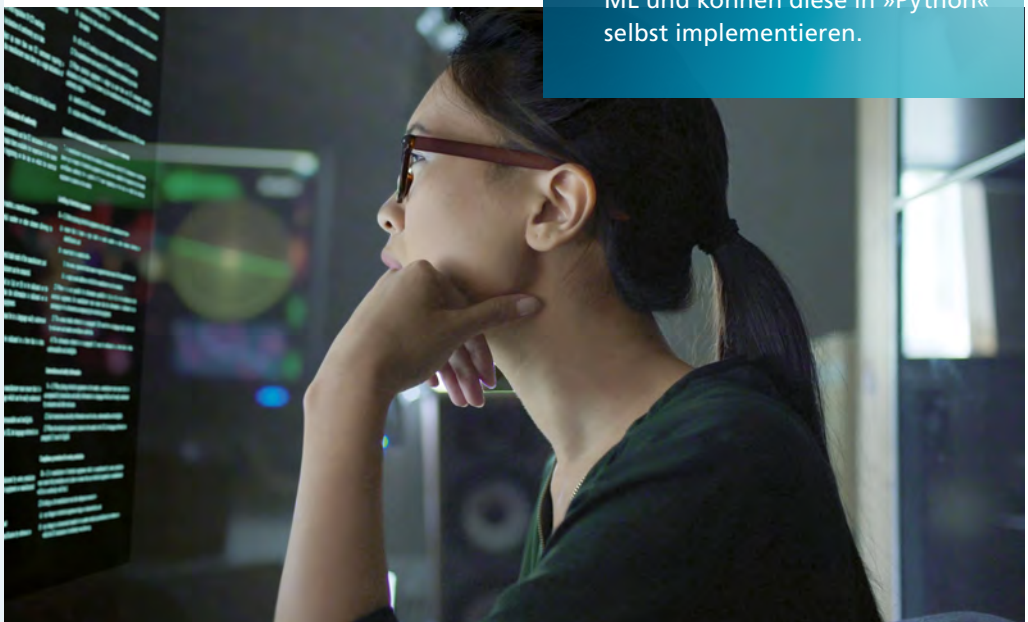
Musterlösungen zur Nachbereitung

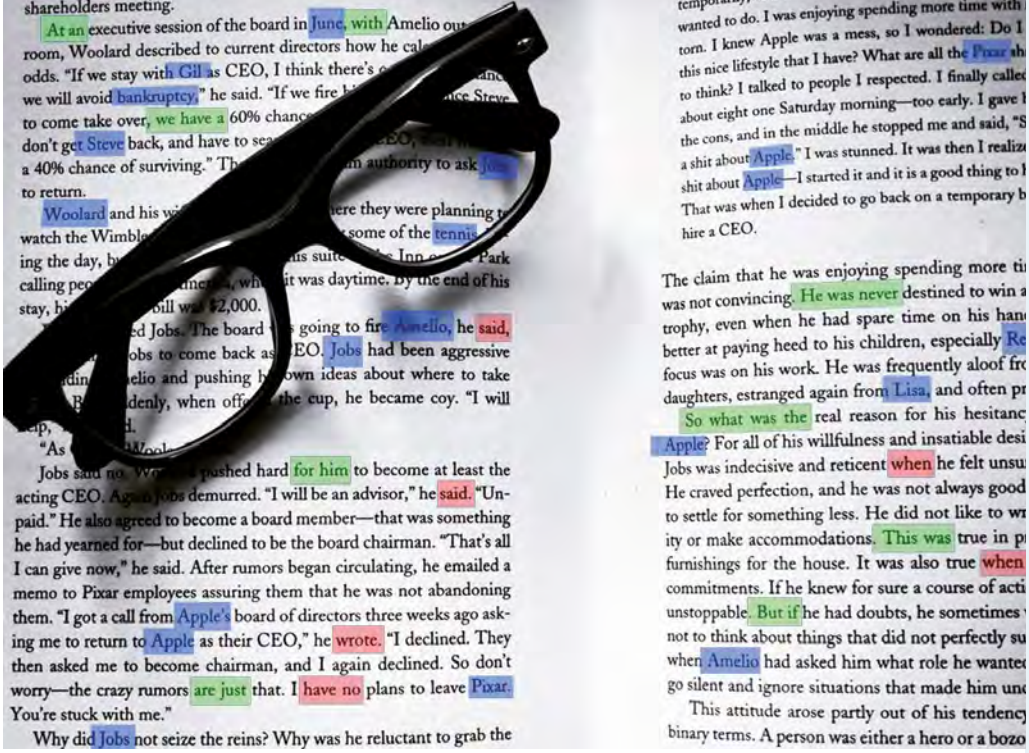
Tipps zu Literatur und Software

Die Programmierübungen bearbeiten Sie online auf unserem Jupyter-Server (CoCalc-Umgebung) in Ihrem eigenen Browser. Keine Installation bei Ihnen benötigt!

Ihr Nutzen

- Nach dem Seminar verstehen Sie moderne Verfahren des NLP und ML und können diese in »Python« selbst implementieren.





shareholders meeting.
At an executive session of the board in June, with Amelio out
room, Woolard described to current directors how he ca
odds. "If we stay with Gil as CEO, I think there's
we will avoid bankruptcy," he said. "If we fire
to come take over, we have a 60% chanc
don't get Steve back, and have to sea
a 40% chance of surviving." Th
to return.
Woolard and his w
watch the Wimble
ing the day, b
calling peo
stay, h
Jobs said no.
acting CEO. A
paid." He also agreed to become a board member—that was something
he had yearned for—but declined to be the board chairman. "That's all
I can give now," he said. After rumors began circulating, he emailed a
memo to Pixar employees assuring them that he was not abandoning
them. "I got a call from Apple's board of directors three weeks ago ask-
ing me to return to Apple as their CEO," he wrote. "I declined. They
then asked me to become chairman, and I again declined. So don't
worry—the crazy rumors are just that. I have no plans to leave Pixar.
You're stuck with me."
Why did Jobs not seize the reins? Why was he reluctant to grab the

authority to ask
ere they were planning
some of the tenni
Park
it was daytime. By the end of his
bill was $2,000.
d Jobs. The board
going to fire Amelio, he said,
obs to come back as
EO. Jobs had been aggressive
elio and pushing h
own ideas about where to take
denly, when offe
the cup, he became coy. "I will
pushed hard for him to become at least the
Jobs demurred. "I will be an advisor," he said. "Un-

wanted to do. I was enjoying spending more time with
torn. I knew Apple was a mess, so I wondered: Do I
this nice lifestyle that I have? What are all the Pixar sh
to think? I talked to people I respected. I finally calle
about eight one Saturday morning—too early. I gave
the cons, and in the middle he stopped me and said, "S
a shit about Apple." I was stunned. It was then I realiz
shit about Apple—I started it and it is a good thing to
That was when I decided to go back on a temporary b
hire a CEO.

The claim that he was enjoying spending more ti
was not convincing. He was never destined to win a
trophy, even when he had spare time on his han
better at paying heed to his children, especially Re
focus was on his work. He was frequently aloof fr
daughters, estranged again from Lisa, and often pr
So what was the real reason for his hesitanc
Apple? For all of his willfulness and insatiable desi
Jobs was indecisive and reticent when he felt unsu
He craved perfection, and he was not always good
to settle for something less. He did not like to w
ity or make accommodations. This was true in p
furnishings for the house. It was also true when
commitments. If he knew for sure a course of acti
unstoppable. But if he had doubts, he sometimes
not to think about things that did not perfectly su
when Amelio had asked him what role he wante
go silent and ignore situations that made him un
This attitude arose partly out of his tendency
binary terms. A person was either a hero or a bozo

Thematische Exploration von Textdaten mit Topic Modeling

»Schürfen« in Textdaten (Aufbaukurs)

Die Herausforderung: Bei der computergestützten Analyse von Textdaten stößt man häufig auf Fragestellungen wie »Wer hat diesen Text verfasst?« oder »Welche Themen und Inhalte stecken in meinen Textdaten?« Hierzu bieten wir Ihnen zwei (getrennt buchbare) Aufbaukurse zur Schreibstil-Analyse oder zum Topic Modeling – und zwar zur Theorie und zur Praxis in Python.

Inhalte des Seminars

Einführung in Topic Modeling

Latent Dirichlet Allocation (LDA)

Bibliothek pyLDAvis

BERT

HDBSCAN

UMAP

- viele Livedemos zu den Kursthemen
- Python-Programmierübungen als Jupyter-Notebooks
- intensive Online-Betreuung durch unsere Expertinnen und Experten
- Quellcode-Beispiele für Sie zur Nachbereitung
- Tipps zu Literatur und Software

Die Programmierübungen bearbeiten Sie online auf unserem Jupyter-Server (CoCalc-Umgebung) in Ihrem eigenen Browser. Keine Installation bei Ihnen benötigt!

Ihr Nutzen

- Nach dem Seminar verstehen Sie moderne Verfahren der Autorschaftsanalyse und/oder des Topic Modeling und können diese in »Python« selbst implementieren.

IT-Forensik | **Online**

Informationen im Überblick

Gute Kenntnisse in Python-Programmierung sowie NLP und ML (siehe S. 9)

Forensiker*innen, Ermittler*innen, Data Scientists/ Analysts, IT-Sicherheitsexpert*innen, Data Journalists, Social Media Manager, PR-Beratung, Financial Analysts

6 Stunden

500,–

online

Veranstaltet durch

Fraunhofer SIT

Referent*innen:

Jeong-Eun Choi,
wiss. Mitarbeiterin,
Fraunhofer SIT

Inna Vogel,
wiss. Mitarbeiterin,
Mediensicherheit
und IT-Forensik,
Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/topic-modeling-LDA

Informationen im Überblick

Allgemeine IT-Kenntnisse

Ermittelnde, Forensiker *innen, Beauftragte für IT-Sicherheit oder Compliance, Fachjournalist*innen, IT-affine Interessierte

17 Stunden an 4 Tagen

1200,–

online

Veranstaltet durch

Fraunhofer SIT

Referent*innen:

Florian Platzer,
wiss. Mitarbeiter
Fraunhofer SIT

Alexandra Lux,
wiss. Mitarbeiterin,
TU Darmstadt

Sandra Wittmer,
wiss. Mitarbeiterin,
TU Darmstadt

York Yannikos,
stv. Abteilungsleitung
Mediensicherheit u
nd IT-Forensik,
Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/darknet

Einführung in Darknet und Kryptowährungen

Das Tor-Netzwerk und Bitcoin verstehen

Im Darknet kann man inkognito kommunizieren, ohne Spuren zu hinterlassen, und Kryptowährungen ermöglichen anonymen Handel. Andererseits gestatten diese Technologien illegale Aktivitäten im Schutz der Anonymität. Dieses Spannungsfeld zwischen Freiheit und Sicherheit ist ein sensibles Thema und aktueller denn je. In unserem Kurs werden Sie mit diesen Themen vertraut gemacht, um Chancen und Bedrohungen etwa durch das Tor-Netzwerk oder Bitcoin zu verstehen.

Inhalte des Seminars

Einführung
- Definitionen: Was sind Darknet, Clearnet und Deepweb?
- Technologie des »Internets« und des Tor-Netzes
- Motivation: Wer braucht das Darknet? Wozu?

Kommunikation im Darknet
- Soziale Netze
- Nutzerkompetenz

Inhalte im Darknet
- Statistiken über Inhalte in Tor (legal, illegal)

Rechtliche Perspektiven auf das Darknet
- Grundrechte
- Strafrecht

Kryptowährungen
- Kryptographiegrundlagen und die »Blockchain«
- Das Bitcoin-Zahlungssystem und andere Währungen
- Methoden der Geldwäsche (Mixer)

Livedemos bzw. Praxisübungen an Ihrem eigenen PC
- Tor-Browser und Suche im Darknet
- Hidden Service installieren

Ihr Nutzen

- Nach dem Seminar können Sie Wege der Darknet-Kommunikation besser nachvollziehen und beurteilen.
- Sie können einschätzen, welche Informationen hierbei relevant/irrelevant sind.
- Sie lernen anhand praxisnaher Übungen den Umgang mit dem Tor-Netzwerk.
- Sie erhalten eine neutrale, unverfälschte Sicht auf das Darknet und Kryptowährungen.

Open Source Intelligence (OSINT) für Behörden

Aktuelle Tools kennenlernen

Die Recherche nach digitalen Spuren und Indizien im Zusammenhang mit einer möglichen Straftat bildet heutzutage einen zentralen Bestandteil der Fallarbeit. Diese kann mithilfe von OSINT-Maßnahmen unterstützt und vervollständigt werden. Dabei können Analysten und Bearbeiter auf verschiedene Webseiten und Tools zurückgreifen. Durch die sich permanent verändernden Rahmenbedingungen bei der Informationsbeschaffung müssen die Anwendenden in der Lage sein, sich anzupassen und eigenständig entstehende Probleme zu lösen.

Inhalte des Seminars

Tag 1
- Session 1: Einführung OSINT
- Session 2: Grundlegende Ausstattung
- Session 3: Informationsgewinnung mit Google & Co.
- Session 4: spezielle Suchmaschinen
- Session 5: Recherche in sozialen Netzwerken
- Session 6: Suche im Darknet

Tag 2
- Session 1: Digitale Medien
- Session 2: Kartendienste und GIS
- Session 3: Kommunikationsplattformen
- Session 4: Dokumente
- Session 5: Linux für OSINT
- Session 6: Informationsbeschaffung (Maltego)

Ihr Nutzen

- Nach dem Seminar sind Sie in der Lage, Informationen systematisch zusammenzustellen.
- Sie können relevante Abläufe entwickeln und umsetzen.
- Sie lernen, Gefahren zu erkennen, einzuschätzen und gegebenenfalls neu zu bewerten.
- Sie können digitale Beweismittel finden und sichern.

Informationen im Überblick

Problemloser Umgang mit dem PC sowie IT-Grundkenntnisse

Das Modul richtet sich gezielt an Personen aus kriminologischen Institutionen und Behörden

2 Tage Präsenz

1200,–

Mittweida

Veranstaltet durch

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Referent:

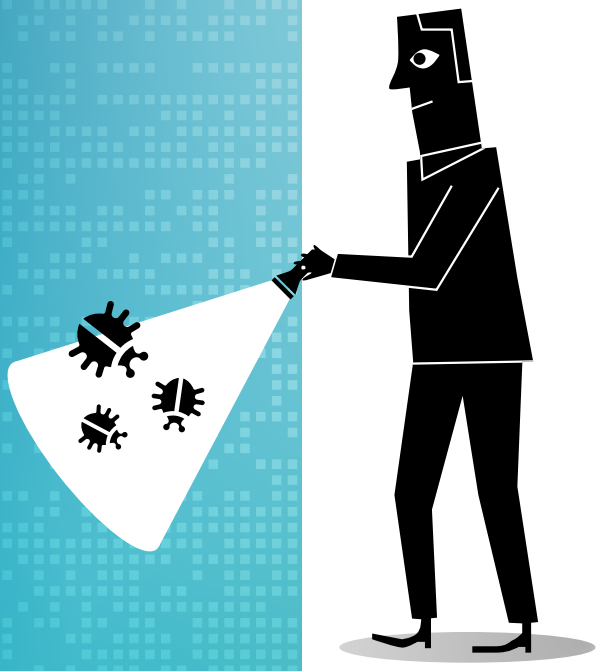
Martin Klöden, seit 2018 Trainer im LLCS HSMW

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.raunhofer.de/osint-fuer-behoerden

Schadsoftware- & Firmwareanalyse

Schadsoftware muss jederzeit kritisch beleuchtet werden



Schadsoftware gehört zu den negativen Begleiterscheinungen wachsender Digitalisierungsprozesse. Gerade durch IoT hat sich das Bedrohungspotenzial in diesem Bereich stark erhöht, denn IoT-Geräte vergrößern die Angriffsfläche für Schädlinge exponentiell. Darüber hinaus zeigen sich in der Analyse stetig neue Herausforderungen.

Der gängige Ansatz im Vorgehen bestand in der Identifikation der bösartigen Software. Doch nur zu wissen, dass ein Programm sich möglicherweise bösartig verhält oder nicht, reicht nicht mehr aus! Moderne Schadsoftware ist dazu in der Lage, sich unkenntlich zu machen, um ihre Analyse hinauszuzögern. Aber auch grundlegende Analysen wie die exakte Bestimmung von Malware können schnell zur Herausforderung werden, die gesichertes Spezialwissen benötigt. Automatisierte Werkzeuge können zwar Arbeit abnehmen, jedoch ersetzen Sie keine vollumfassende Analyse von Experten.

Schwachstellen können schnell zu Problemen im Unternehmen führen. Cyberangreifer nehmen mehr und mehr Bereiche in den Fokus. Sie nutzen die zusätzlichen Angriffsflächen durch mobile Endgeräte und IoT bewusst aus. Schnelles Handeln und eine aufwendige, detaillierte Analyse der Schadsoftware von geschulten Analystinnen und Analysten hilft, Schadenspotenziale abzuwägen und konkrete Gefahren abzuwehren.

Im Lernlabor Cybersicherheit werden Sie bedarfsgerecht auf die aktuelle Bedrohungslage vorbereitet. Sie profitieren von wissenschaftlicher Expertise, die nicht nur gegenwärtige Probleme in den Blick nimmt, sondern auch aktuelle Trends beleuchten kann. In unseren Seminaren erfahren Sie, wie Angreifer vorgehen, und wie Sie Ihr Unternehmen im Ernstfall am besten schützen. Das Lernlabor bietet Ihnen eine Brücke zwischen wissenschaftlicher Erkenntnis und unternehmensgerechten Ansätzen.

Workshop-Reihe

IT-Sicherheit im »Internet of Things«

Die einzelnen Module sind bedarfsgerecht aufgebaut, sodass Sie in demjenigen Level und Schulungsmodul einsteigen können, welches für Ihre Vorkenntnisse und Kompetenzbedarfe geeignet ist.

Einführung in die Firmwareanalyse

Sicherheitslücken erkennen

Internet of Things und Industrie 4.0 lassen die Anzahl vernetzter Geräte deutlich ansteigen. Jedes dieser in das Internet verbundenen Geräte kann als Angriffsvektor für Manipulationen dienen. Zum nachhaltigen Schutz eines Systems, sog. Firmware, ist es daher nötig, genau über die verwendeten Systeme im Bilde zu sein, alle vernetzten Komponenten auf dem neuesten Stand zu halten und das Verwenden unsicherer Komponenten zu erkennen und zu vermeiden.

- Praktische Übungen zum Entpacken der Firmwarecontainer, um einzelne Komponenten wie Web- oder Samba-Server zu identifizieren
- Analyse der Firmwarekomponenten anhand statischer und dynamischer Analysemethoden erproben

Einführung in die Benutzung der wichtigsten Werkzeuge für Firmwareextraktion und -analyse

Inhalte des Seminars

Übersicht Firmware
- Aufbau und Betriebssysteme kennen und verstehen
- Beschaffung von Firmware über Hersteller oder Geräteschnittstellen

Extraktion
- Nicht invasive Firmware-Extraktion verstehen und erproben
- Teilinvasive Firmwareextraktion verstehen und erproben
- Invasive Firmwareextraktion verstehen und erproben

Entpacken und initiale Analyse
- Angriffsvektoren auf Embedded Devices verstehen

Ihr Nutzen

- Nach dem Seminar können Sie Firmware aus den meisten Geräten extrahieren.
- Sie lernen, Firmware in vielen Fällen zu entpacken.
- Sie können initiale toolgestütze Analyse von Firmware durchführen.
- Sie können einschätzen, wie viel Sorgfalt der Hersteller bei der Entwicklung der Firmware walten ließ.

Schadsoftware- & Firmwareanalyse | Präsenz

Informationen im Überblick

Grundkenntnisse im Umgang mit Linux und der Kommandozeile

Analyst*innen, Entwickler*innen, Reverser, Sicherheitsexpert*innen

2 Tage Präsenz

1200,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referenten:

Johannes vom Dorp, Forschungsgruppenleiter Applied System Analysis Fraunhofer FKIE

Christopher Krah, IT-Sicherheitsforscher, Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/einfuehrung-firmwareanalyse

Informationen im Überblick

- Grundkenntnisse im Umgang mit Linux und der Kommandozeile; Kenntnisse über grundlegende Firmwareanalysemethoden
- Analyst*innen, IT-Forensiker*innen, Reverser
- 2 Tage Präsenz
- 1200,–
- Bonn

Veranstaltet durch

Fraunhofer FKIE

Referenten:

Johannes vom Dorp, Forschungsgruppenleiter Applied System Analysis Fraunhofer FKIE

Christopher Krah, IT-Sicherheitsforscher, Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/fortgeschrittene_firmwareanalyse

Fortgeschrittene Firmwareanalyse

Komplexe Analyseverfahren anwenden

Wie in anderen Bereichen der IT scheitern automatisierte Werkzeuge zur Firmwareanalyse regelmäßig an bislang unbekannter Firmware. Die Diversität von Firmware geht dabei auf die Vielfalt der eingesetzten Hardware sowie fehlende Standardisierung zurück. Um beliebige Firmware analysieren zu können, muss ein Analyst in der Lage sein, die automatisierten Verfahren zu erweitern oder die Firmware zunächst in ein bereits bekanntes Format zu bringen. Allgemeine Werkzeuge decken zudem nur generelle Probleme mit Firmware auf, während manuelle Analysen spezifischere und teilweise kritischere Probleme in Firmware identifizieren können. Geräte mit hohen Sicherheitsstandards haben außerdem Mechanismen, um Firmware zu schützen und damit die Analyse zu verhindern. Diese Mechanismen können teilweise durch eine direkte Analyse der Hardware erkannt und ausgehebelt werden.

Inhalte des Seminars

Reverse Engineering von Firmware-Komponenten

Praktische Übungen von statischer Analyse an realer Firmware

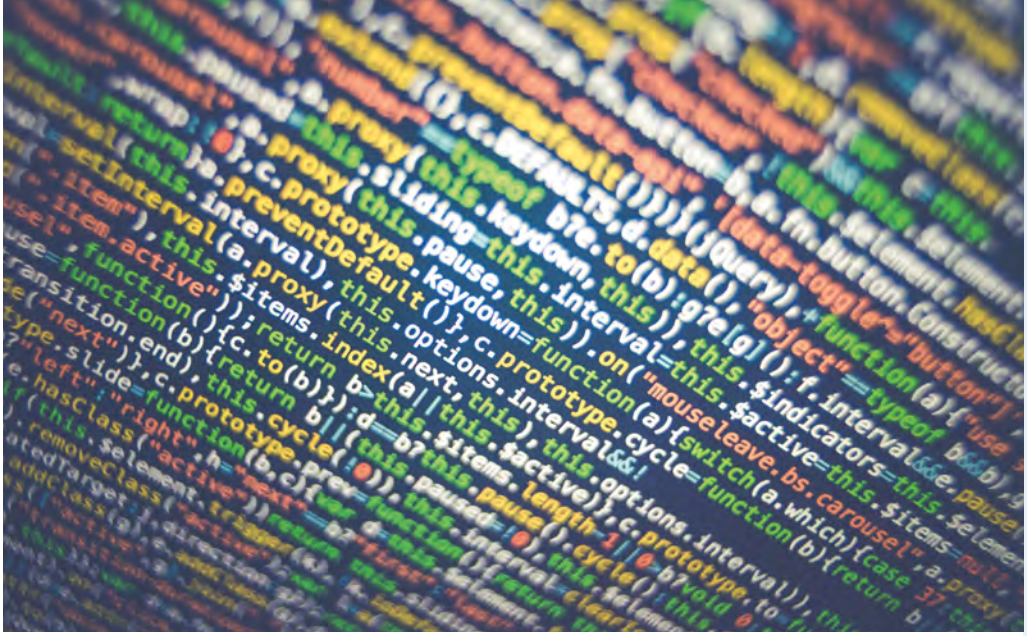
Fuzzing auf ganzer Firmware oder auf Firmware-Komponenten

Ausnutzen von Sicherheitslücken für die Einrichtung von Firmware-Backdoors/ -Rootkits

Entwicklung neuer automatisierter Analyseverfahren

Ihr Nutzen

- Nach dem Seminar können Sie fortgeschrittene manuelle Analysen an realer Firmware durchführen.
- Sie können eigene Analysen in automatisierte Werkzeuge integrieren.
- Sie sind in der Lage, fortgeschrittene Analysen auf Hardwareebene durchzuführen.



Grundlagen Schadsoftware-analyse Windows

Malware untersuchen und verstehen lernen

Die Herausforderung: Erkennen der Schadsoftware und ihrer Funktionalität. Oft ist es nicht mehr ausreichend, nur festzustellen, ob sich ein Programm potenziell bösartig verhält oder nicht. Allein die exakte Bestimmung einer Malwarefamilie kann bereits eine Herausforderung sein, denn Malware liegt üblicherweise nur als fertig kompiliertes Programm im Maschinencode vor. Da nun also der Quellcode nicht verfügbar ist, sind schnell Spezialwissen wie auch Werkzeuge erforderlich, um Erkenntnisse über Fähigkeiten und Verhalten der Malware zu erarbeiten.

Inhalte des Seminars

Generelle Einführung zu Schadsoftware: Relevante Beispiele und die grundsätzliche Analysemethodik des Reverse Engineerings

Systemnahe Einführung zu Windows und der Umgang mit Virtualisierung als Schutzschicht

Oberflächliche Analysen durch Systembeobachtung

Überblick über die x86-/x64-Architektur und ein Schnellkurs zum Verständnis von Assemblern

Einführung in dynamische und statische Analysetechniken mit der Gelegenheit, diese im Rahmen von Botnet Takeovers in unserer Laborumgebung zu vertiefen

Ihr Nutzen

- Nach dem Seminar können Sie Angriffsvektoren von Schadsoftware besser einschätzen.
- Sie können Analysen durchführen, um einen grundsätzlichen Eindruck von Schadsoftware zu erhalten.
- Sie kennen typische Analysetools wie Debugger und IDA Pro und können diese anwenden.

Schadsoftware- & Firmwareanalyse | **Präsenz**

Informationen im Überblick

Grundlegendes Verständnis der Funktionsweise des Internets; Verständnis von Netzwerkprotokollen (TCP/ IP) und Netzwerkprogrammierung. Grundlegende Programmierkenntnisse sind empfehlenswert

Administrator*innen, Analyst*innen, CERT-Mitarbeitende

3 Tage Präsenz

1800,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Daniel Plohmann, IT-Sicherheitsforscher, Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/grundl-schadsoftwareanalyse-windows

Informationen im Überblick

Theoretische und praktische Kenntnisse in der Analyse von Windows-Schadsoftware sowie Netzwerkkenntnisse; Umgang mit Windows/Linux; Umgang mit IDA Pro und Debugger (z. B. x64dbg); Verständnis von x86-Assembler; Programmierkenntnisse in Python (C/C+ vorteilhaft)

Administrator*innen, Analyst*innen, CERT-Mitarbeitende

2 Tage Präsenz

1200,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Niklas Bergmann,
IT-Sicherheitsforscher,
Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/fortgeschrittene-schadsoftwareanalyse-windows

Fortgeschrittene Schadsoftwareanalyse Windows

Verschleierungstechniken erkennen und auflösen

Moderne Schadsoftware versucht, ihre Analyse durch die Verwendung von verschleiernden Techniken hinauszuzögern. Dynamisches Entpacken von Code, Verschlüsselung von Strings und Code-Injektionen sind nur einige der genutzten Techniken. Diese Techniken zielen sowohl auf die dynamische als auch auf die statische Analyse ab. Sofern die Detailanalyse einer bestimmten Schadsoftware angestrebt wird, muss ein Schadsoftwareanalyst in der Lage sein, diese Techniken zu identifizieren und anschließend zu entschleiern, damit eine Schadsoftwareanalyse überhaupt möglich ist.

Inhalte des Seminars

Manuelles Entpacken von Programmen mit anschließender IAT-Rekonstruktion

Manuelles Entpacken von schadsoftwarespezifischen Packern

Härten einer virtuellen Maschine

Erkennung und Umgehung von Code-Injektionen

Automatisierung von IDA Pro mittels IDAPython und Sark

Erkennung und Umgehung von Stringverschlüsselung

Erkennung und Umgehung von API-Verschleierung

Ihr Nutzen

- Nach dem Seminar können Sie Verschleierungsmethoden erkennen und bewerten.
- Sie können einfache Verschleierungsmethoden selbst programmatisch auflösen.
- Anhand vieler praxisnaher Übungen mit aktueller und relevanter Schadsoftware lernen Sie Techniken zu Erkennung und Auflösen von Verschleierungsmethoden kennen.

Hier erhalten Sie aktuelles Wissen!

Aktuelle Informationen zu unseren Seminarangeboten, Veranstaltungen und Themen im Bereich Cybersicherheit finden Sie hier:

www.cybersicherheit.fraunhofer.de

Stöbern Sie in unserem Blog und erfahren Sie, was unsere Fachexpertinnen und -experten über aktuelle Themen im Bereich Cybersicherheit berichten:

www.cybersicherheit.fraunhofer.de/de/blog

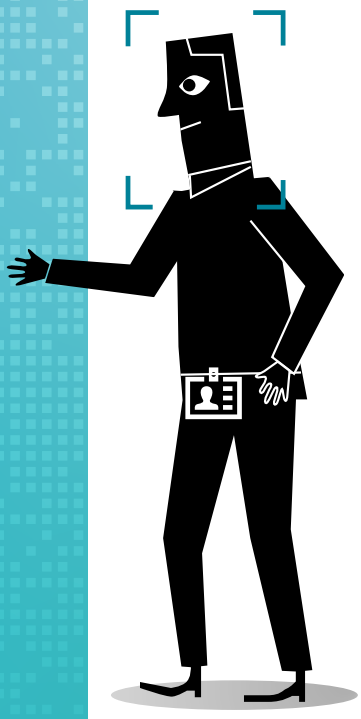
Abonnieren Sie unseren Newsletter und bleiben Sie so auf dem Laufenden:

www.cybersicherheit.fraunhofer.de/newsletter

Weitere Informationen rund um das Thema Weiterbildung bei der Fraunhofer Academy erhalten Sie hier:

Identitäten & Identitätsnachweis

Sicherheit setzt ein vertrauenswürdiges Identitätsmanagement voraus



Auch im Unternehmen bilden sich im Zuge der Digitalisierung neue Herausforderungen für ein vertrauenswürdiges Identitätsmanagement. Stetig wachsende Bedrohungsmöglichkeiten stehen neuen technischen Lösungskonzepten gegenüber: Biometrische Verfahren machen Authentifizierungen von Personen noch eindeutiger, digitales Identitätsmanagement ermöglicht mehr Absicherung. Doch wo liegen die Grenzen solcher Verfahren, wo entstehen rechtliche Problemstellungen, und welche technischen Anforderungen bringen neue Technologien mit sich?

Reibungslose Unternehmensprozesse sind wesentlich davon abhängig, Identitäten im Firmennetz eindeutig zuordnen zu können. Im Austausch mit anderen Firmen oder externen Mitarbeitern steigert sich die Relevanz eindeutiger Authentifizierung erheblich. Auch der stetig wachsende Einsatz von mobilen Endgeräten oder IoT erhöht die Komplexität des Identitätsmanagements und stellt Unternehmen so vor neue Herausforderungen. Gerade im Kontext internationaler Prozesse können EU-Verordnungen problematisch werden!

Im Lernlabor Cybersicherheit lernen Sie, welche Chancen und Risiken in gegenwärtigen Authentifizierungsverfahren liegen. In unseren Seminaren erfahren Sie, wie Sie sich im professionellen, aber auch im persönlichen Bereich schützen können. Sie bekommen Einblicke in biometrische Verfahren, OAuth, OpenID oder FIDO, und welche Protokolle relevant sind.

Bauen Sie ein vertrauenswürdiges Identitätsmanagement mit dem Know-how zu rechtlich-organisatorischen Rahmenbedingungen und den fachlich-technischen Anforderungen auf.

Digitale Identitäten

Verstehen, Bewerten, Anwenden

Die Herausforderung: Firmenübergreifende Systemzugriffe sicher machen. Digitale Identitäten sind selbstverständlich im Unternehmensablauf. Dabei geht es nicht nur um die Koordinierung interner Mitarbeiterinnen und Mitarbeiter, sondern auch um den Austausch mit Firmen, Zulieferern und Externen. Techniken wie OAuth und Multi-Faktor-Authentifizierung rücken dann in den Fokus. Auf internationaler Ebene kann das jedoch zu Problemen führen. Dieses Seminar bietet Ihnen einen Überblick über föderiertes Identitätsmanagement. Lernen Sie, Digitale Identitäten zu verstehen und zu bewerten.

Inhalte des Seminars

Identitätsmanagement, Authentifizierung und rechtliche Komponenten
- Übergreifendes Identitätsmanagement: Protokolle SAML, OAuth, OAuth Extensions und OpenID Connect
- Mit Praxisbeispielen und Übungen zu jedem Themenbereich

Offene und lizenzfreie Standards der FIDO-Allianz
- Weltweite Authentifizierung und schnelle Identitäten bei digitalen Verbindungen
- Zwei-Faktor-Authentifizierung Universal Second Factor (U2F)

Bedeutung der EU-Verordnungen
- Elektronischer Identitäten- und Datenschutz

Ihr Nutzen

- Nach dem Seminar haben Sie einen umfassenden Überblick über relevante Protokolle und Randbedingungen zum Thema Digitale Identitäten.
- Sie haben durch Übungen und Diskussionen gelernt, Entscheidungen zum Identitätsmanagement in Ihrem Unternehmen zu treffen.
- Sie verfügen über aktuelles Wissen zu aktuellen Protokollen und Trends (z. B. OpenID-Connect, Fido, Online-Ausweisfunktion).

Informationen im Überblick

Keine Voraussetzungen

Anwender*innen, Sicherheitskräfte, Fachkräfte, Spezialist*innen, Webentwickler*innen, Betreiber*innen von internen Diensten

2 Tage Präsenz

1200,–

Berlin

Veranstaltet durch

Fraunhofer AISEC

Referenten:

Prof. Dr. Marian Margraf, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/digitale-identiaeten

Inhouse- oder Firmen- und Behördenschulungen

Inhouse-Schulungen individuell auf Sie zugeschnitten

Wollen Sie Inhalte aus unserem Kursangebot individuell zusammenstellen, oder finden Sie in unserem Angebot keinen passenden Termin oder Ort? Kein Problem: Stellen Sie Ihre ganz persönlichen Bedürfnisse in den Vordergrund.

Sie haben die Wahl, so geht's:

- Wählen Sie ein Wunschseminar aus unseren vielfältigen Themen aus und bestimmen Sie den Zeitraum und Schulungsort.
- Nennen Sie uns Inhalte aus unseren Kursangeboten, die geschult werden sollen, und wir konzipieren ein passendes Seminar.
- Sie sagen uns, welches spezielle Wissen geschult werden soll, und wir entwickeln eine individuelle Schulung für Sie.

Bei einem individuellen Inhouse-Seminar erhalten Sie genau auf Ihre Bedürfnisse abgestimmtes Wissen – für Ihr Unternehmen, Abteilungen Ihres Unternehmens, für Ihre Behörde, Fachreferate oder einzelne Mitarbeiterinnen und Mitarbeiter. Dabei stehen wir Ihnen sehr gerne beratend zur Verfügung, wenn es um für Sie maßgeschneiderte, inhaltliche Zusammenstellung der vielfältigen Kombinationsmöglichkeiten unserer Themen geht.

Wir als Lernlabor Cybersicherheit bieten Ihnen alle relevanten Elemente aus einer Hand: Die didaktische, mediale sowie technische Umsetzung der Inhalte, aber auch Konzept und Umsetzung.

Fragen Sie uns an!

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne

telefonisch unter +49 89 1205-1555

e-mail: cybersicherheit@fraunhofer.de

www.cybersicherheit.fraunhofer.de

Möchten Sie Informationen zu einem anderen Themengebiet?

Hier finden Sie alle Broschüren rund um die Weiterbildungen im Lernlabor Cybersicherheit: www.cybersicherheit.fraunhofer.de/downloads

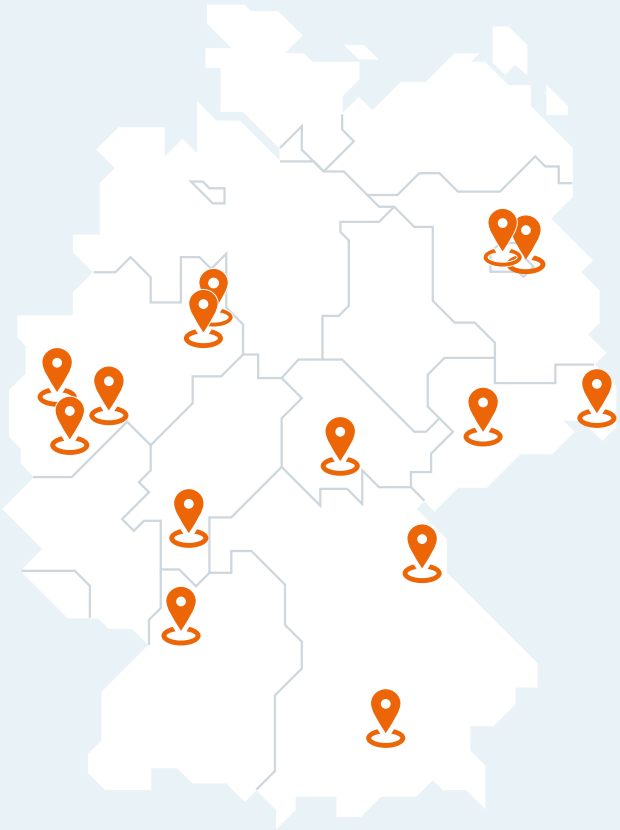
Aktuelle Qualifizierung aus der angewandten Forschung

Das Lernlabor Cybersicherheit ist ein Weiterbildungsprogramm, in dem Expertinnen und Experten von Fraunhofer und ausgewählten Fachhochschulen aktuellste Erkenntnisse auf dem Gebiet der Cybersicherheit vermitteln. Die Lehrmodule werden von den beteiligten Fraunhofer-Instituten und Fachhochschulen entwickelt und weitergegeben. Die Fraunhofer Academy ist die Geschäftsstelle und Plattform der Initiative, die Entwicklung, Vermarktung, Teilnehmermanagement und Qualitätssicherung koordiniert. Das Programm wird durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Die beteiligten Partnerhochschulen

- Ostbayerische Technische Hochschule Amberg-Weiden
- Hochschule für Technik und Wirtschaft Berlin
- Hochschule Bonn-Rhein-Sieg
- Hochschule Mittweida
- Hochschule Niederrhein
- Technische Hochschule Ostwestfalen-Lippe
- Hochschule Zittau/Görlitz

Standorte der Lern- und Forschungslabore der beteiligten Fraunhofer-Institute und Fachhochschulen



Die beteiligten Fraunhofer-Institute

- Fraunhofer AISEC
- Fraunhofer FKIE
- Fraunhofer FOKUS
- Fraunhofer IEM
- Fraunhofer IOSB
- Fraunhofer IOSB-AST
- Fraunhofer IOSB-INA
- Fraunhofer SIT

Know-how schafft Sicherheit! Seit 5 Jahren unterstützen wir deshalb Unternehmen auf dem Weg zu mehr IT-Sicherheit.«

Dr. Raphaela Schätz,
Qualitäts- und Programm Management
im Lernlabor Cybersicherheit

Herausgeber

Fraunhofer Academy
Hansastraße 27c
80686 München

Telefon +49 89 1205-1555
Fax +49 89 1205-77-1599

cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Redaktion: Elly Leimenstoll

Layout und Satz, Illustrationen:
Vierthaler & Braun

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne
- telefonisch unter + 49 89 1205-1555
- per E-Mail: cybersicherheit@fraunhofer.de
- auf unserer Website unter

www.cybersicherheit.fraunhofer.de

Wir beraten Sie gerne, welche Weiterbildungen und Inhalte für Sie hilfreich sind.

Sie suchen nach Angeboten für Ihr Team?

Für Unternehmen bieten wir Inhouse-Schulungen und unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung. Wir erheben gemeinsam mit Ihnen den Kompetenzbedarf in Ihrer Abteilung oder Firma und beraten Sie, die richtigen Fähigkeiten in Ihrer Organisation aufzubauen.

Adem Salgin

Ihr Ansprechpartner im Lernlabor Cybersicherheit

Seminarberatung
und Anmeldung

Stand Mai 2022

Sie erreichen uns

– telefonisch unter +49 89 1205-1555
– per E-Mail: cybersicherheit@fraunhofer.de
– auf unserer Website unter

www.cybersicherheit.fraunhofer.de