

DUALER BACHELORSTUDIENGANG

AI CYBER SECURITY B. Sc.

ENTERPRISE INTEGRATED

Cybersecurity studieren. In der Welt, in der Cybersecurity tatsächlich stattfindet.

Das Profil verbindet Informatik, AI und Security mit der Realität moderner Unternehmen: Cloud, Identitäten, Netzwerke, Security Operations und verantwortliche Umsetzung.



WAS DIESES PROFIL IM UNTERNEHMEN LEISTET

- **AI Security & Security Operations**
- **Network & Cloud Cyber Security**
- **Identity & Zero Trust**
- **SOC, SIEM & Threat Intelligence**

Junior Security Analyst · SOC Analyst · Cloud Security Specialist

AI stärkt die Verteidigung – und schafft zugleich neue Angriffsflächen.

Unternehmen brauchen Menschen, die beide Seiten verstehen und in ihrer realen Systemlandschaft beherrschen.

01 AI FOR SECURITY

Anomalien erkennen, Threat Intelligence verdichten und Reaktionen automatisieren.

02 SECURITY FOR AI

Modelle, Daten und Agenten gegen Manipulation, Leakage und Missbrauch schützen.

03 ENTERPRISE-KOMPLEXITÄT

Cloud, Netzwerk, Identitäten, Endpoints und Prozesse zusammen absichern.

04 HANDLUNGSFÄHIGKEIT

Vorfälle bewerten, priorisieren und unter Zeitdruck verantwortlich handeln.



DIE KONSEQUENZ

Security-Kompetenz entsteht nicht durch Zuschauen.

Sie entsteht dort, wo Wissen auf reale Systeme, Entscheidungen und Verantwortung trifft.

Was Cybersecurity-Spezialisten im Unternehmen tatsächlich tun.

01

ANGRIFFE ERKENNEN & ANALYSIEREN

Signale korrelieren, Risiken einordnen und aus Daten belastbare Hinweise gewinnen.

02

SYSTEME & IDENTITÄTEN SCHÜTZEN

Cloud, Netzwerke, Zugriffe und digitale Identitäten konsequent absichern.

03

SECURITY OPERATIONS AUTOMATISIEREN

Detection, Response und wiederkehrende Abläufe mit AI wirksamer machen.

04

VORFÄLLE BEWERTEN & VERANTWORTEN

Priorisieren, kommunizieren und Maßnahmen strukturiert in den Betrieb bringen.

Fünf Security-Disziplinen. Eine integrierte Enterprise-Perspektive.

Der Studiengang verbindet Informatik, AI, Security Operations und reale Unternehmensarchitekturen.

01 AI SECURITY & SECOPS

AI für Erkennung und Reaktion einsetzen – und AI-Systeme selbst schützen.

02 NETWORK & CLOUD SECURITY

Architekturen, Workloads und Daten über hybride Umgebungen absichern.

03 IDENTITY & ZERO TRUST

Identitäten, Berechtigungen und Zugriffe konsequent verifizieren.

04 SOC, SIEM & THREAT INTELLIGENCE

Signale bündeln, Bedrohungen bewerten und Detection verbessern.

05 ENDPOINT, XDR & INCIDENT RESPONSE

Endgeräte schützen, Vorfälle untersuchen und Reaktionen orchestrieren.

06 GOVERNANCE & COMMUNICATION

Risiken übersetzen, Entscheidungen dokumentieren und Maßnahmen verankern.

Aus Grundlagen wird Enterprise-Security-Kompetenz.

Drei Lernschichten bauen aufeinander auf: verstehen, spezialisieren, anwenden und verantworten.

01

AKADEMISCHER CORE

FUNDAMENT

Verstehen

Informatik & Netzwerke
Cloud & Kryptografie
Secure Coding
Machine Learning & AI Engineering

02

ENTERPRISE-TRACKS

2–3 VON 5

Spezialisieren

AI Security & SecOps
Network & Cloud Security
Identity & Zero Trust
SOC, SIEM & Threat Intelligence
Endpoint, XDR & Incident Response

03

PRAXIS & ABSCHLUSS

4 BAUSTEINE

Anwenden und verantworten

Labs und Cyber Ranges
Projektstudium im Unternehmen
Praxisphase
Bachelor Thesis

FORTLAUFEND: Future Skills · Business English · Praxistransfer · Security Mindset

Führende Technologiepartner und Enterprise-Technologien werden dort integriert, wo sie fachlich zur Kompetenzentwicklung beitragen.

Verantwortung wächst mit jedem Trimester.

42 MONATE · 180 ECTS · BACHELOR OF SCIENCE · START
OKTOBER 2027

3 + 2

**Wissen wird in derselben Woche
im Unternehmen angewendet.**

Jede Woche: zwei Tage Hochschule und drei Tage Unternehmen

1 TAG
HOCHSCHULE

1 TAG
HOCHSCHULE

1 TAG
UNTERNEHMEN

1 TAG
UNTERNEHMEN

1 TAG
UNTERNEHMEN

KEIN LERNEN AUF VORRAT

**Neue Methoden fließen direkt in Aufgaben,
Projekte und Security-Entscheidungen ein.**

PHASE 1 · VERSTEHEN

Systeme, Angriffe und Schutzprinzipien einordnen

Informatik, Netzwerke, Cloud, Kryptografie, Secure Coding und AI fundiert aufbauen.

PHASE 2 · SPEZIALISIEREN

Enterprise-Technologien praktisch beherrschen

Zwei bis drei Tracks wählen, in Labs und Cyber Ranges anwenden und vertiefen.

PHASE 3 · VERANTWORTEN

Reale Security-Probleme im Unternehmen lösen

Use Cases umsetzen, Entscheidungen vertreten und das Bachelorprojekt im Unternehmenskontext abschließen.

DIE ZIELROLLE IM UNTERNEHMEN

Welche Cybersecurity-Kompetenz soll in Ihrem Unternehmen entstehen?

Security Analyst · SOC Analyst · Cloud Security Specialist · Identity & Zero Trust Specialist · Threat Intelligence & SIEM Specialist

Lassen Sie uns Aufgaben, Technologieumfeld und zukünftige Verantwortung der dual Studierenden gemeinsam schärfen.

IHR ANSPRECHPARTNER

Christopher Pilz

Geschäftsführer
gotoitcareer GmbH

SÜDCAMPUS BAD HOMBURG

Am Weidenring 4
61352 Bad Homburg

christopher.pilz@gotoitcareer.com

www.gotoitcareer.de

**Nicht nur Cyber Security
studieren. Cyber Security
können.**