2. MSc Cybersecurity

a) Pflichtmodule

<table>
<tr><td colspan="5">HPI-CS-T: Security Technologies</td><td>Anzahl der Leistungspunkte (LP): 6</td></tr>
<tr><td>Modulart (Pflicht- oder Wahlpflichtmodul):</td><td colspan="5">Pflichtmodul</td></tr>
<tr><td>Inhalte und Qualifikationsziele des Moduls:</td><td colspan="5"><u>Inhalt:</u>
Die fortschreitende Digitalisierung der Gesellschaft führt dazu, dass digitale Systeme immer relevanter werden und deswegen auch deren Schutz einen immer höheren Stellwert einnimmt. Dieses Modul vermittelt einen Überblick über generelle Sicherheitsgefahren und wie diese mittels entsprechender Methoden analysiert werden können, um das Risiko abzuschätzen. Dabei werden auch die verschiedenen Typen von Angreifern sowie deren Motivation näher betrachtet. Darüber hinaus werden in dem Modul verschiedene bekannte aber auch neuartige Konzepte vermittelt (z. B. Least Privilege, Defense in Depth, Mutual Authentication, Awareness), die genutzt werden können, um ein entsprechendes Risiko zu verringern bzw. ganz zu eliminieren.

<u>Qualifikationsziele:</u>
Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen.
Die Studierenden…
● verstehen aktuelle Sicherheitsgefahren und können deren Risiko bewerten;
● kennen die Eigenschaften und die Motivation von verschiedenen Angreifertypen;
● besitzen ein umfassendes Verständnis von verschiedenen Sicherheitskonzepten und deren Einfluss auf entsprechende Sicherheitsrisikos;
● erweitern ihre fachliche Urteilskompetenz;
● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen;
● erweitern ihre Lernfähigkeiten;
● wissen, welche Probleme im Themenbereich Security Concepts derzeit offen sind;
● haben Einblicke in aktuelle Lösungsansätze in Industrie- und Forschungsprojekten und in den aktuellen Stand der Forschung gewonnen.</td></tr>
<tr><td>Modul(teil)prüfungen (Anzahl, Form, Umfang):</td><td colspan="5">Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.)</td></tr>
<tr><td>Selbstlernzeit (in Zeitstunden (h)):</td><td colspan="5">120</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="2">Veranstaltungen (Lehrformen)</td><td>Kontaktzeit (in SWS)</td><td colspan="2">Prüfungsnebenleistungen (Anzahl, Form, Umfang)</td><td rowspan="2" colspan="2">Lehrveranstaltungsbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)</td></tr>
<tr><td></td><td>Für den Abschluss des Moduls</td><td>Für die Zulassung zur Modulprüfung</td></tr>
<tr><td>Vorlesung (Vorlesung)</td><td>3</td><td>-</td><td>-</td><td colspan="2">-</td></tr>
<tr><td>Übung (Übung)</td><td>1</td><td>-</td><td>Übungsaufgaben (50%)</td><td colspan="2"></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="2">Häufigkeit des Angebots:</td><td colspan="4">Wintersemester</td></tr>
<tr><td colspan="2">Voraussetzung für die Teilnahme am Modul:</td><td colspan="4">Keine</td></tr>
<tr><td colspan="2">Angaben zur Gefährdungsbeurteilung:</td><td colspan="4">Belegung für Schwangere unproblematisch</td></tr>
<tr><td colspan="2">Anbietende Lehreinheit:</td><td colspan="4">Digital Engineering (HPI)</td></tr>
</table>

HPI-CS-C: Advanced Cryptography	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Pflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt:** Sowohl Unternehmen als auch private Personen erzeugen, übertragen und speichern eine immer größer werdende Menge an sensiblen und kritischen Daten. Daher steigt auch die Relevanz diese Daten mit geeigneten Methoden zu schützen. In diesem Modul werden verschiedene kryptographische Primitiven sowie deren korrekte Verwendung in komplexen Systemen und Protokollen vermittelt. Dabei werden neben gängigen und zurzeit verwendeten kryptographischen Algorithmen auch Algorithmen aus dem Bereich Post-Quanten-Kryptographie und Quantenkryptographie näher betrachtet. Darüber hinaus werden verschiedene Methoden der Kryptoanalyse behandelt. **Qualifikationsziele:** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● besitzen ein umfassendes Verständnis der Eigenschaften verschiedener kryptographischer Primitiven (z. B. asymmetrische und symmetrische kryptographische Verfahren, kryptographische Hashfunktionen); ● können die Sicherheit von komplexen Systemen und Protokollen auf Grundlage der verwendeten kryptographischen Algorithmen bewerten und Schwachstellen identifizieren; ● sind in der Lage auf theoretischer Ebene sichere Systeme und Protokolle zu designen – unter Verwendung der entsprechenden kryptographischen Primitiven; ● erlangen fachspezifische theoretische, methodische und praktische Kenntnisse; ● können für die Lösung von Problemen selbständig geeignete Informationsquellen erschließen und einzusetzen; ● wissen, welche Probleme im Themenbereich Kryptographie derzeit offen sind; ● haben Einblicke in aktuelle Lösungsansätze in Industrie- und Forschungsprojekten und in den aktuellen Stand der Forschung gewonnen.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung (Vorlesung)	3	-	-	-
Übung (Übung)	1	-	Übungsaufgaben (50%)	

Häufigkeit des Angebots:	Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

<table>
<tr><th colspan="5">HPI-CS-S: Systems and Network Security</th><th>Anzahl der Leistungspunkte (LP): 6</th></tr>
<tr><td colspan="2">Modulart (Pflicht- oder Wahlpflichtmodul):</td><td colspan="4">Pflichtmodul</td></tr>
<tr><td colspan="2">Inhalte und Qualifikationsziele des Moduls:</td><td colspan="4"><u>Inhalt:</u>
Eine steigende Anzahl von Angriffen versucht einzelne Systeme oder auch vernetzte Infrastrukturen zu kompromittieren. Deshalb werden in diesem Modul zunächst die relevanten Charakteristika von verschiedenen Systemen und Netzwerken betrachtet, um Angriffsvektoren bzw. potentielle Schwachstellen zu identifizieren und zu kategorisieren. Dies ermöglicht es im Anschluss verschiedene theoretische Sicherheitskonzepte und -maßnahmen zu betrachten, sowie deren praktische Umsetzung für konkrete Angriffsvektoren zu untersuchen. Neben den verwendeten Sicherheitskonzepten und entsprechenden Schwachstellen von „klassischen“ Computer-Systemen und -Netzwerken, befasst sich dieses Modul auch mit den Sicherheitsfunktionen und möglichen Verwundbarkeiten von Systemen – wie zum Beispiel Smartphones, IoT-Geräten und Cloud Infrastrukturen – sowie auch von aufkommenden Netzwerktechnologien – wie zum Beispiel 5G.

<u>Qualifikationsziele:</u>
Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen.

Die Studierenden…
● kennen relevante Charakteristika/ Sicherheitskonzepte von gängigen Systemen und Netzwerken, sowie potentielle Schwachstellen;
● sind in der Lage selbstständig Systeme und Netzwerke mit entsprechenden Methoden auf theoretischer Ebene zu analysieren und potentielle Angriffsvektoren zu identifizieren;
● können beschriebene Sicherheitsmaßnahmen im Kontext verschiedener Bedrohungen/Angriffe evaluieren;
● erwerben Erfahrung im Umgang mit Systemen und Werkzeugen die es ermöglichen Sicherheitsmaßnahmen zu analysieren und potentielle Angriffsvektoren zu identifizieren;
● wissen, welche Probleme im Themenbereich Systems and Network Security relevant und derzeit offen sind;
● haben Einblicke in aktuelle Lösungsansätze in Industrie- und Forschungsprojekten und in den aktuellen Stand der Forschung gewonnen.</td></tr>
<tr><td colspan="2">Modul(teil)prüfungen (Anzahl, Form, Umfang):</td><td colspan="4">Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.)</td></tr>
<tr><td colspan="2">Selbstlernzeit (in Zeitstunden (h)):</td><td colspan="4">120</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="2">Veranstaltungen (Lehrformen)</td><td rowspan="2">Kontaktzeit (in SWS)</td><td colspan="2">Prüfungsnebenleistungen (Anzahl, Form, Umfang)</td><td rowspan="2">Lehrveranstaltungsbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)</td></tr>
<tr><td>Für den Abschluss des Moduls</td><td>Für die Zulassung zur Modulprüfung</td></tr>
<tr><td>Vorlesung (Vorlesung)</td><td>3</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Übung (Übung)</td><td>1</td><td>-</td><td>Übungsaufgaben (50%)</td><td></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="2">Häufigkeit des Angebots:</td><td colspan="4">Wintersemester</td></tr>
<tr><td colspan="2">Voraussetzung für die Teilnahme am Modul:</td><td colspan="4">Keine</td></tr>
<tr><td colspan="2">Angaben zur Gefährdungsbeurteilung:</td><td colspan="4">Belegung für Schwangere unproblematisch</td></tr>
<tr><td colspan="2">Anbietende Lehreinheit:</td><td colspan="4">Digital Engineering (HPI)</td></tr>
</table>

HPI-CS-A: Application Security	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Pflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt:** Softwaresysteme werden für eine stetig steigende Zahl von Aufgaben eingesetzt. Dies führt dazu, dass diese Systeme immer komplexer werden und damit auch die Absicherung dieser Softwaresysteme immer relevanter wird. Dieses Modul thematisiert Methoden und Ansätze zur Entwicklung von sicheren Anwendungen (z. B. Secure Coding und Security by Design). Darüber hinaus werden unterschiedliche Sicherheitsmaßnahmen für zum Beispiel Web-Anwendungen, Apps für Smartphones/ Tablets sowie klassische Anwendungen betrachtet. Außerdem behandelt dieses Modul verschiedene Analysemethoden, die es ermöglichen, Schwachstellenklassen sowie entsprechende Angriffsvektoren auf theoretischer aber auch praktischer Ebene zu identifizieren und zu analysieren. **Qualifikationsziele:** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● verstehen die Herausforderungen der Entwicklung von sicheren und hochkomplexen Softwaresystemen; ● kennen gängige Sicherheitsmaßnahmen und -konzepte für verschiedene Kategorien von Anwendungen; ● kennen mögliche Analysemethoden zu Identifizierung und Analyse von Schwachstellen sowie Angriffsmöglichkeiten und können diese entsprechend einsetzen; ● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen; ● erwerben Erfahrung im Umgang mit Analysesystemen und -werkzeugen; ● wissen, welche Probleme im Themenbereich Anwendungssicherheit derzeit offen sind; ● haben Einblicke in aktuelle Lösungsansätze in Industrie- und Forschungsprojekten und in den aktuellen Stand der Forschung gewonnen.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung (Vorlesung)	3	-	-	-
Übung (Übung)	1	-	Übungsaufgaben (50%)	

Häufigkeit des Angebots:	Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-CS-PE: Data Protection & Ethics	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Pflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Dieses Modul vermittelt relevante Datenschutzaspekte, die im Rahmen der Analyse von Daten und der Identifizierung von Schwachstellen bzw. Angriffen wichtig sind. Insbesondere die europäische Datenschutz-Grundverordnung und verwandte Vorschriften sind dabei zu beachten. Darüber hinaus bietet das Modul einen Überblick über ethische Fragen in Bezug auf die technische Entwicklung und die Gesellschaft seit der Industrialisierung. Gegenstand ist die Stellung des Menschen in der Gesellschaft insbesondere unter dem Aspekt der modernen Datenverarbeitung im Kontext von Cybersecurity. Lernziel ist es, die durch die Verarbeitung von (personenbezogenen) Daten hervorgerufenen Konfliktsituationen in Wirtschaft und Gesellschaft datenschutzrechtlich und ethisch bewerten zu können und solche Situationen präventiv zu vermeiden. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlangen fachspezifische theoretische, methodische und praktische Kenntnisse; ● erlernen, den datenschutzrechtlichen und ethischen Rahmen für die Nutzung und Analyse von Daten im Kontext von Cybersecurity in Wirtschaft und Gesellschaft zu ermessen und zu beurteilen; ● erweitern ihre fachliche Urteilskompetenz; ● können zu datenschutzrechtlichen und ethischen Fragen geeignete Lösungskonzepte und -strategien auswählen und anwenden; ● sammeln Erfahrung in der Formalisierung und Abstraktion von Problemstellungen; ● erlernen Ansätze von Führungsfähigkeiten; ● üben Konfliktfähigkeit im Team.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Hausarbeit (mind. 10 Seiten) zusammen mit Ergebnispräsentation (Vortrag, 30 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung (Vorlesung)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-CS-L: Security Lab	**Anzahl der Leistungspunkte (LP): 12**
Modulart (Pflicht- oder Wahlpflichtmodul):	Pflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Im Security Lab bearbeiten die Studierenden gemeinsam in einer Gruppe eine ausgewählte forschungsbezogene Frage aus einem Fachgebiet der Cybersecurity. Die Fragestellung wird analysiert, für einen Teilbereich wird eine Lösung entworfen, diese konstruktiv umgesetzt und wissenschaftlich dokumentiert. Die Lösungen werden permanent auf ihre Stärken und Schwächen evaluiert. Die Evaluierung mit anderen Ansätzen bzw. Methoden vertieft außerdem das praktische Verständnis dieser. Die Studierenden erlangen dadurch tiefe Einblicke in die aktuelle Forschungsarbeit in den Fachgebieten und beteiligen sich an der Entwicklung neuer Lösungen. Dieses Modul vertieft die wissenschaftliche Ausbildung der Studierenden. Die Security-Lab-Tätigkeit findet arbeitsteilig in Projektgruppen von in der Regel jeweils mindestens drei Mitgliedern statt. Security Labs werden von Prüfungsberechtigten geleitet. **Qualifikationsziele** In diesem Modul sollen Kenntnisse aus fortgeschrittenen Cybersecurity-Modulen in die Praxis umgesetzt werden. Die Studierenden… ● erlernen die eigenständige Entwicklung von Cybersecurity-Werkzeugen zur sicherheitstechnischen Analyse von Systemen, Netzwerken und Anwendungen oder Werkzeugen für die Speicherung, Verwaltung, Analyse und Visualisierung von großen und komplexen Daten aus dem Security-Kontext; ● werden befähigt Cybersecurity-Analysesysteme als Lösungen für konkrete Anwendungen anzupassen und zu entwickeln und diese vergleichend zu evaluieren; ● erlangen durch die Arbeit in Teams Kompetenzen im Bereich des Projektmanagements; ● gewinnen Souveränität in der kollaborativen und arbeitsteiligen Bearbeitung von Aufgabenstellungen; ● trainieren Team-, Kommunikations- und Konfliktfähigkeit; ● lernen die systematische Auseinandersetzung mit Forschungsfragestellungen.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Hausarbeit von mindestens 12 Seiten zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 30-45 Min.); zur Hausarbeit gehören die Implementierungsarbeiten zur Lösung der Forschungsfragestellung
Selbstlernzeit (in Zeitstunden (h)):	240

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Projekttätigkeit (Projekt)	8	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

b) Wahlpflichtmodule
Vertiefungsgebiet Security Analytics

HPI-SECA-K: Security Analytics – Konzepte und Methoden	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Immer größere und vielfältigere Datenbestände, wie zum Beispiel Ereignisdaten, Threat Intelligence und Open Source Intelligence, sind relevant für die Erkennung von Angriffen und von potentiellen Risiken im Kontext von Cybersecurity. Die Herausforderung besteht darin entsprechende Techniken und Konzepte zu verwenden, damit diese Daten in effizienter und umfassender Art und Weise analysiert werden können. Das Vertiefungsgebiet Security Analytics betrachtet alle notwendigen Schritte, welche das Sammeln der Daten, das Normalisieren bzw. Aufbereiten der Daten, die entsprechenden analytischen Methoden und Konzepte sowie die Visualisierung der Ergebnisse umfassen. Dieses Modul vermittelt die grundlegenden Konzepte und Methoden von Security Analytics wie beispielsweise Data Exploration, Streaming, ETL (Extract, Transform, Load), Korrelation, überwachtes Lernen und unüberwachtes Lernen. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlangen Kenntnisse zur Analyse großer und vielfältiger Datenbestände im Kontext von Cybersecurity und entsprechender Analysetechniken; ● können umfassende Datenbestände sammeln, normalisieren/ aufbereiten, analysieren und Ergebnisse visualisieren; ● besitzen ein umfassendes Verständnis von verschiedenen Security Analytics-Konzepten und können diese erläutern; ● können unterschiedliche Methoden zur Analyse großer und vielfältiger Datenbestände hinsichtlich ihrer Wirksamkeit und Anwendbarkeit einschätzen und vergleichen; ● verstehen, welche Probleme im Themenbereich Security Analytics derzeit offen sind und haben Einblick in den diesbezüglichen Stand der Forschung gewonnen.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-SECA-T: Security Analytics – Techniken und Werkzeuge	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Das Modul vermittelt vertieftes praktisches Wissen im Bereich Security Analytics mithilfe gängiger Security-Analytics-Systeme und -Werkzeuge. In Anlehnung an etablierte Datenanalyse-Prozesse, wie zum Beispiel ETL oder Streaming in Verbindung mit verschiedenen analytischen Ansätzen, werden Praxisbeispiele für die Erkennung von Angriffen und potentiellen Risiken im Kontext von Cybersecurity untersucht. Dabei werden neben verschiedenen statistischen Analyseansätze und Korrelationsansätzen auch Machine Learning Verfahren, wie beispielsweise Clustering, Klassifikation und Deep Learning, vermittelt. Darüber hinaus werden die Stärken und Schwächen für die einzelnen Schritte und Analyseverfahren näher betrachtet. Die Studierenden werden zudem für offene Forschungsprobleme sensibilisiert und entwickeln eigene Techniken und Werkzeuge zur Lösung dieser Forschungsfragen. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlernen die Anwendung verschiedener Analysetechniken und -werkzeuge – statistische Ansätze, Korrelation und Machine Learning; ● erlernen die praktische Anwendung von Security Analytics-Methoden und -Systemen; ● können Verfahren zur Erkennung von Angriffen und potentiellen Risiken praktisch anwenden; ● werden befähigt gängige Softwarewerkzeuge einzusetzen, Rohdaten zu sammeln, zu normalisieren/ aufzubereiten, strukturiert zu analysieren und Ergebnisse zu visualisieren; ● können zu einer vorgegebenen Problemstellung geeignete Lösungskonzepte und -strategien auswählen und anwenden; ● erweitern ihre fachliche Urteilskompetenz; ● können etablierte Prozesse zur Datenanalyse im Kontext von Cybersecurity für verschiedene Anforderungen implementieren und parametrieren; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-SECA-S: Security Analytics - Spezialisierung	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Das Modul vermittelt aktuelle Forschungsfragestellungen und -ergebnisse aus dem Bereich Cybersecurity im Vertiefungsgebiet Security Analytics. Im Modul liegt der Fokus auf der Identifikation von Schwächen des aktuellen Stands der Forschung und der wissenschaftlichen Erarbeitung weiterführender Methoden und Systeme im Bereich Security Analytics. Es werden offene Forschungsfragen wie zum Beispiel Integration von Threat Intelligence und Open Source Intelligence, Verwendung von Deep Learning-Verfahren und Optimierung von bereits eingesetzten Verfahren betrachtet. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erarbeiten Limitierungen und Erweiterungen bestehender Security-Analytics-Methoden und -Systeme; ● behandeln aktuelle Forschungsfragen zum Beispiel Integration von Threat Intelligence und Machine Learning im Kontext von Cybersecurity; ● erlernen die wissenschaftliche Bearbeitung aktueller Forschungsfragestellungen im Bereich Security Analytics; ● lernen die eigenständige Nachbearbeitung eines Themas auf Grundlage von Primär- und Sekundärliteratur; ● erlernen selbständig relevante Fachliteratur zu identifizieren, zu erschließen und die Inhalte anzuwenden; ● werden befähigt ungelöste Probleme aus der Forschung selbstständig zu bearbeiten und Lösungen dazu zu entwickeln; ● erlernen die Präsentation und kritische Diskussion bearbeiteter Aufgaben; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten; ● entwickeln Diskussionsvermögen und -techniken.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Empfohlen wird die vorangehende Teilnahme an HPI-SECA-K oder HPI-SECA-T.
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

Vertiefungsgebiet Identity Management

HPI-IDMG-K: Identity Management – Konzepte und Methoden	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Um die Sicherheit von Systemen und Daten gewährleisten zu können, ist es erforderlich, dass nur berechtigte Personen bzw. Systeme auf entsprechende Ressourcen zugreifen können. Im Kontext von Cybersecurity befasst sich das Vertiefungsgebiet Identity Management mit der gesamtheitlichen Betrachtung verschiedener Ansätze und Methoden, mithilfe derer diese Anforderung erfüllt werden kann. Der Fokus dieses Moduls liegt in der Vermittlung von theoretischen Konzepten und Methoden, die zum Beispiel für die Authentifizierung und Autorisierung verwendet werden können. Außerdem werden Ansätze vermittelt, mit denen es möglich ist, die verschiedenen Stärken und Schwächen der einzelnen Methoden zu identifizieren. Ein weiterer Schwerpunkt dieses Moduls ist die Betrachtung verschiedener praktischer Anwendungsszenarien, in denen die vorher erläuterten Ansätze verwendet werden, beispielsweise Kerberos, SAML und OAuth. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlernen Konzepte und Methoden die beispielweise für die Authentifizierung und Autorisierung verwendet werden; ● können praktische Anwendungsszenarien und die entsprechend verwendeten Konzepte und Methoden evaluieren; ● können zu einer vorgegebenen Problemstellung geeignete Lösungskonzepte und -strategien auswählen und anwenden; ● erweitern ihre fachliche Urteilskompetenz; ● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen; ● lernen entsprechende Analysemethoden kennen; ● können Strategien zur Vorverarbeitung für verschiedene Anforderungen bewerten; ● erkennen komplexe Probleme des Identitätsmanagements und sind in der Lage entsprechende Lösungsstrategien zu entwickeln; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgenden Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-IDMG-T: Identity Management - Techniken und Werkzeuge	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Dieses Modul behandelt Techniken und Werkzeuge, die zum Identitätsmanagement in komplexen Systemen genutzt werden können. Insbesondere werden dabei Techniken und Werkzeuge beispielsweise auf ihre Fähigkeiten, anwendungsspezifische Nutzbarkeit und Praktikabilität untersucht. Im Zuge dessen sollen z. B. auch konkrete Implementierungen wichtiger Technologien und Ansätze aus dem Bereich Identitätsmanagement wie etwa Public Key Infrastructure, auf Blockchain basierte Ansätze und behavior-based Authentication betrachtet werden. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlernen verschiedene Ansätze, die im Bereich Identitätsmanagement von komplexen Systemen Anwendung finden; ● können Technologien wie beispielsweise Blockchain und behavior-based Authenication, welche zum Identitätsmanagement eingesetzt werden, evaluieren und anwenden; ● können zu einer vorgegebenen Problemstellung geeignete Lösungskonzepte und -ansätze auswählen und anwenden; ● erweitern ihre fachliche Urteilskompetenz; ● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen; ● können verschiedene Ansätze aus dem Bereich Authentifizierung und Autorisierung entsprechend der vorgegebenen Anforderungen implementieren; ● erlangen einen Überblick über die verfügbaren Techniken und Werkzeuge und lernen diese zu bewerten; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-IDMG-S: Identity Management – Spezialisierung	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Dieses Modul behandelt relevante Teilaspekte, die zum Identitätsmanagement in komplexen Systemen notwendig sind und setzt hierbei den Schwerpunkt auf aktuelle Forschungsfragestellungen und -ergebnisse. Dabei wird für Themen wie zum Beispiel Authentifizierung, Autorisierung, Blockchain oder behavior-based Authentication der aktuelle Forschungsstand reflektiert betrachtet und im Detail untersucht. Jüngste Entwicklungen in Wissenschaft und Industrie aus dem Identitätsmanagement-Bereich dienen als Ausgangspunkt und werden näher betrachtet. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erarbeiten Limitierungen und Erweiterungen bestehender Identitätsmanagement-Methoden und -Systeme; ● behandeln aktuelle Forschungsfragen zum Beispiel aus den Bereichen Authentifizierung und Autorisierung; ● erlernen die wissenschaftliche Bearbeitung aktueller Forschungsfragestellungen im Bereich Identitätsmanagement; ● lernen die eigenständige Nachbearbeitung eines Themas auf Grundlage von Primär- und Sekundärliteratur; ● erwerben Erfahrung im Umgang mit Softwaresystemen und -werkzeugen; ● können bearbeitete Aufgaben präsentieren und gegen kritische Einwände verteidigen; ● haben einen tiefen und präzisen Einblick in den praktischen Einsatz hochaktueller Identitätsmanagementtechnologien und -systeme; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten; ● entwickeln Diskussionsvermögen und -techniken.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.).
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Empfohlen wird die vorangehende Teilnahme an HPI-IDMG-K oder HPI-IDMG-T.
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

Vertiefungsgebiet Cyber Attack and Defense

HPI-CYAD-K: Cyber Attack and Defense - Konzepte und Methoden	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Angreifer verändern und entwickeln die eingesetzten Angriffskonzepte und -methoden ständig weiter, um vorhandene Sicherheitssysteme und -mechanismen umgehen zu können. Daraus begründet sich auch die Notwendigkeit eingesetzte Systeme zur Erkennung und Verhinderung von Angriffen ebenfalls ständig zu verbessern. Dieses Modul vermittelt sowohl Konzepte und Methoden für den Angriff also auch für die Verteidigung von Systemen und komplexen Infrastrukturen. Dabei werden die relevanten Phasen eines Angriffs, wie zum Beispiel Reconnaissance, Initial Compromise, Lateral Movement und Command and Control, betrachtet sowie die üblicherweise verwendeten Methoden. Darüber hinaus werden für die eingesetzten Angriffsmethoden entsprechende Analyse- und Erkennungsansätze vorgestellt durch die ein Angriff in der entsprechenden Phase identifiziert werden kann. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden… ● erlernen Konzepte und Methoden für den Angriff und die Verteidigung von Systemen und komplexen Infrastrukturen; ● können eingesetzte Angriffsmethoden evaluieren und entsprechende Analyseansätze einsetzen sowie Erkennungsmethoden nachvollziehen bzw. entwickeln; ● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen; ● können Konzepte und Methoden für die Erkennung von Angriffen und Verteidigungsansätze bewerten; ● erkennen komplexe Probleme der IT-Sicherheit und sind in der Lage Gegenmaßnahmen umzusetzen; ● erweitern ihre Lernfähigkeiten.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-CYAD-T: Cyber Attack and Defense – Techniken und Werkzeuge	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Das Modul vermittelt Techniken und Werkzeuge, die im Bereich Cyber Attack and Defense Verwendung finden. Betrachtet werden dabei verschiedene Ansätze sowie deren Stärken und Schwächen. Es werden beispielsweise Techniken und Werkzeuge zur Sammlung relevanter Informationen, Ausnutzung von Schwachstellen, Umgehung von Sicherheitssystemen und Analyse von Schadsoftware sowie Netzwerkverkehr betrachtet. Auch Konzepte und konkrete Techniken zu Themen wie beispielsweise Lateral Movement, dynamische und statische Analyse, Verschleierung und Signatur- sowie Anomalie-basierte Sicherheitssysteme werden vermittelt. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden... ● haben ein umfassendes Verständnis verschiedener Techniken wie beispielsweise Lateral Movement, dynamische und statische Analyse von Schadsoftware und können diese anwenden; ● können Angriffs- und Verteidigungskonzepte für verschiedene Anforderungen beurteilen und implementieren; ● können zu einer vorgegebenen Problemstellung aus dem Bereich Cyber Attack and Defense geeignete Lösungskonzepte und -strategien auswählen und anwenden; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten; ● sind in der Lage zur Lösung von Problemen selbständig geeignete Informationsquellen zu erschließen und einzusetzen; ● erlangen einen Überblick über die verfügbaren Techniken und Werkzeuge und lernen diese zu bewerten.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Sommersemester, Wintersemester
Voraussetzung für die Teilnahme am Modul:	Keine
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)

HPI-CYAD-S: Cyber Attack and Defense - Spezialisierung	**Anzahl der Leistungspunkte (LP): 6**
Modulart (Pflicht- oder Wahlpflichtmodul):	Wahlpflichtmodul
Inhalte und Qualifikationsziele des Moduls:	**Inhalt** Das Modul vermittelt aktuelle Forschungsfragestellungen und -ergebnisse aus dem Bereich Cyber Attack and Defense. Dabei liegt der Fokus auf der Identifikation von relevanten Schwächen bzw. Einschränkungen des aktuellen Stands der Forschung und der wissenschaftlichen Erarbeitung weiterführender bzw. verbesserter Methoden und Ansätze. Es werden offene Forschungsfragen wie zum Beispiel Verbesserung von Signatur- und Anomalie-basierten Erkennungsansätzen, neuartige Lateral Movement Methoden und neue Ansätze zur Umgehung von Sicherheitsmechanismen behandelt. **Qualifikationsziele** Die Studierenden erwerben detailliertes Wissen über die im Modul gegenständlichen Fachthemen. Die Studierenden … ● erarbeiten Limitierungen und Erweiterungen bestehender Cyber Attack and Defense-Ansätze; ● behandeln aktuelle Cyber Attack and Defense-Methoden, die es ermöglichen neuartige Angriffe zu erkennen oder bestehende Sicherheitssysteme zu umgehen; ● erlernen die wissenschaftliche Bearbeitung aktueller Forschungsfragestellungen im Bereich Cyber Attack and Defense; ● lernen die eigenständige Nachbearbeitung eines Themas auf Grundlage von Primär- und Sekundärliteratur; ● erwerben fachsprachliche Kenntnisse in Englisch; ● erweitern ihre Lernfähigkeiten; ● können bearbeitete Aufgaben präsentieren und gegen kritische Einwände verteidigen; ● haben einen tiefen und präzisen Einblick in den praktischen Einsatz hochaktueller Angriffs- und Verteidigungsmethoden; ● entwickeln Diskussionsvermögen und -techniken.
Modul(teil)prüfungen (Anzahl, Form, Umfang):	Eine Prüfung der folgende Formen: Klausur (90-120 Min.) oder mündliche Prüfung (30-45 Min.) oder Hausarbeit (mind. 8 Seiten) zusammen mit der Präsentation von Forschungsergebnissen (Vortrag, 15-20 Min.)
Selbstlernzeit (in Zeitstunden (h)):	120

Veranstaltungen (Lehrformen)	Kontaktzeit (in SWS)	Prüfungsnebenleistungen (Anzahl, Form, Umfang)		Lehrveranstalbegleitende Modul(teil)prüfung(en) (Anzahl, Form, Umfang)
		Für den Abschluss des Moduls	Für die Zulassung zur Modulprüfung	
Vorlesung/Seminar (Vorlesung oder Seminar)	4	-	-	-

Häufigkeit des Angebots:	Wintersemester, Sommersemester
Voraussetzung für die Teilnahme am Modul:	Empfohlen wird die vorangehende Teilnahme an HPI-CYAD-K oder HPI-CYAD-T.
Angaben zur Gefährdungsbeurteilung:	Belegung für Schwangere unproblematisch
Anbietende Lehreinheit:	Digital Engineering (HPI)