Certificate of Advanced Studies

Security Incident Prevention and Detection

Die Angriffe aus dem Internet werden täglich zahlreicher und raffinierter. Unternehmen sind gezwungen, die Sicherheit ihrer IT-Infrastruktur permanent zu überprüfen und kontinuierlich zu verbessern. Im CAS Security Incident Prevention and Detection lernen Sie, professionell, zielgerichtet und methodisch, Angriffe proaktiv zu verhindern und rasch zu erkennen.

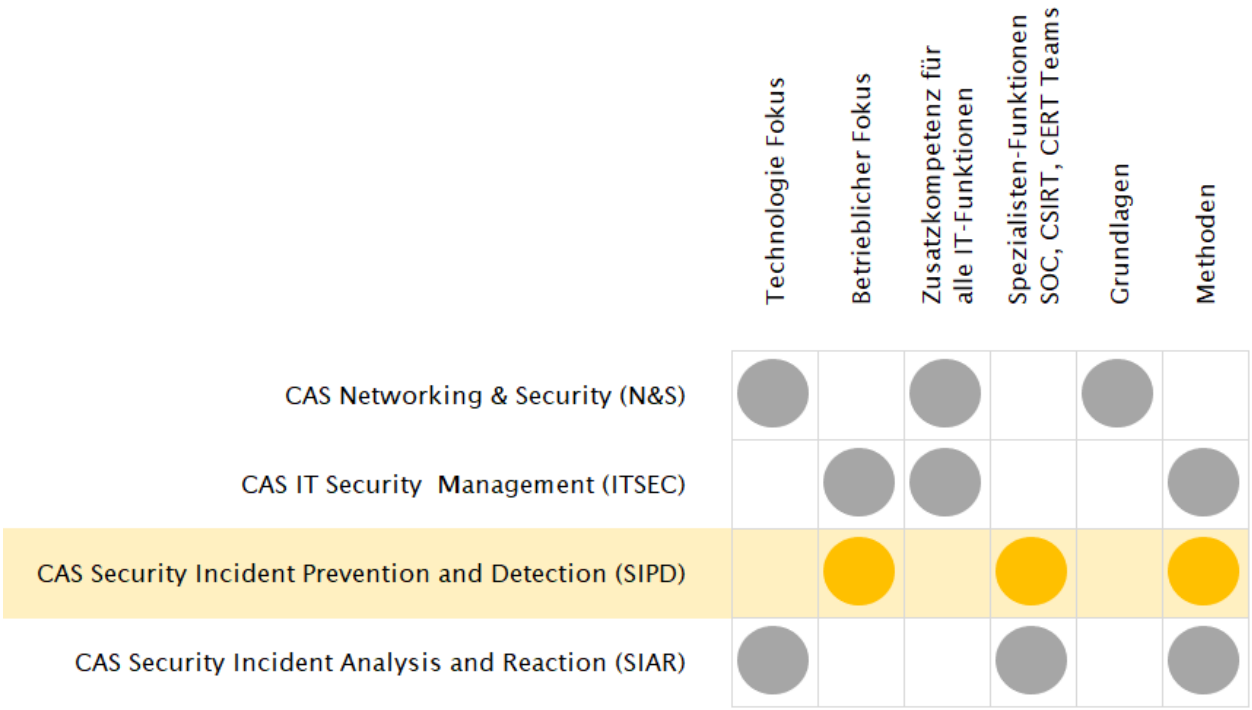
Berner
Fachhochschule

Inhaltsverzeichnis

Stand: 19.09.2024

1 Umfeld

In der heutigen IT-Landschaft lassen sich Sicherheitszwischenfälle nur mit zielgerichteten Massnahmen vermeiden. Je früher Schwachstellen erkannt und je schneller sie behoben sind, umso geringer ist die Gefahr eines erfolgreichen Angriffs. Das CAS Security Incident Prevention and Detection (SIPD) setzt den Fokus auf die Vermeidung und die rasche Erkennung von sicherheitsrelevanten Ereignissen.
Das CAS SIPD ergänzt die beiden CAS «Networking & Security» und «IT Security Management», welche ebenfalls die betrieblichen Seiten beleuchten. Zusammen mit dem weiterführenden CAS Security Incident Analysis and Reaction (SIAR) ergeben die beiden CAS eine umfassende Security-Incident-Management-Ausbildung. Alle vier CAS zusammen bilden eine ideale Ausgangslage für den erfolgreichen Abschluss des MAS Cyber Security.



2 Zielpublikum

Das CAS SIPD richtet sich an IT-Fachkräfte, die in einem Security-, Netzwerk- oder System-Umfeld eine operative Security-Tätigkeit wahrnehmen und IT-Security-Vorfälle verhindern, erkennen und abwenden wollen.

3 Ausbildungsziele

- Sie können Schwachstellen auf verschiedenen Ebenen erkennen, priorisieren und beseitigen.
- Sie kennen wichtige, präventive Schutzmechanismen und können sicherheitsrelevante Meldungen von diesen richtig einordnen und Gegenmassnahmen einleiten.
- Sie können Angriffsversuche schnell erkennen und mit den bestgeeigneten Massnahmen ein weiteres Vordringen der Angreifer verhindern.
- Sie bringen die aus Vorfällen gewonnenen Erkenntnisse wieder in die Verbesserung der IT-Sicherheit ein.

4 Voraussetzungen

- Sie besitzen sehr gute Kenntnisse der Internet-Protokolle und beherrschen mindestens eine Skript- und/oder eine Programmiersprache.
- Sie gehen effizient mit Linux und Windows-Systemen um und kennen die verschiedenen Konfigurationsmöglichkeiten, sowohl für Client wie auch für Server.
- Sie haben bereits einige Erfahrungen mit dem Betrieb und der Konfiguration von Cloud Umgebungen gesammelt (z.B. Azure, AWS).
- Sie bringen IT-Vorkenntnisse im Rahmen einer Informatik- oder Wirtschaftsinformatik-Ausbildung mit. Insbesondere sind Erfahrungen in Projekten der IT-Infrastruktur, Netzwerk-Architektur und/oder IT-Security erforderlich.
- Für das Studium der Fachliteratur und Kursunterlagen werden Englischkenntnisse vorausgesetzt.

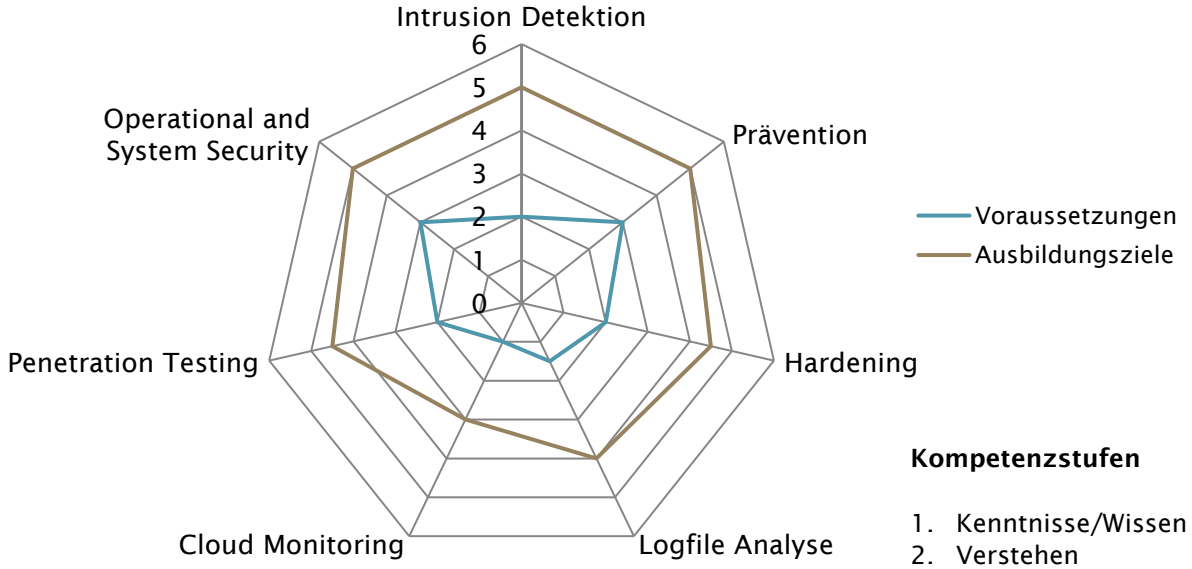
5 Unterrichtssprache

Die Unterrichtssprache ist Deutsch, die Unterlagen sind teilweise in English.

6 Durchführungsort

Berner Fachhochschule, Weiterbildung, Aarbergstrasse 46, 2503 Biel,
Telefon +41 31 848 31 11,
E-Mail weiterbildung.ti@bfh.ch

7 Kompetenzprofil



Kompetenzstufen

1. Kenntnisse/Wissen
2. Verstehen
3. Anwenden
4. Analyse
5. Synthese
6. Beurteilung

8 Kursübersicht

Kurs / Lehreinheit	Lektionen	Stunden	Dozierende
Bedrohung und Operational Security	16		Reto Inversini Mauro Vignati Endre Bangerter
Prävention • Vulnerability- und Patch Management • Malware/Spam Protection • Linux Hardening • Windows und AD Hardening • Cloud Hardening • Penetration Testing • OWASP	68		 Adrian Leuenberger Reto Inversini Reto Inversini Eduard Blenkers Stephan Berger Adrian Leuenberger Dominik Kuhn
Detektion • Logfile Analyse • Network IDS • Host IDS • Cloud Monitoring • Dynamische Malware-Analyse	44		 Heino Kronenberg Reto Inversini Manuel Schilt Stephan Berger Marco Gfeller
Workshop	8		Stefan Egger Heino Kronenberg
Organisation und Meilensteine Semesterarbeit	12		alle
Semester-/Projektarbeit		~ 90	alle
Total	**148**	**~ 90**	

Das CAS umfasst insgesamt 12 ECTS-Credits, was einer Arbeitsleistung von ca. 360h entspricht. Für die einzelnen Kurse ist entsprechend Zeit für Selbststudium, Prüfungsvorbereitung etc. einzurechnen.

9 Didaktik, Präsenz, Distance Learning

Didaktisch ist das CAS geprägt von einer hohen Interaktion zwischen Dozierenden und den Studierenden. Der Theorieteil des Unterrichts wird mit kleinen Aufgaben, Übungen und Diskussionen ergänzt. In der abschliessenden Semesterarbeit soll das im CAS erworbene Wissen an einem konkreten Fall aus dem Umfeld der Studierenden angewendet und die Ergebnisse der Arbeit innerhalb der Klasse in einer Schlusspräsentation weitergegeben werden.

Neben dem klassischen Präsenzunterricht im Klassenzimmer werden einzelne Kursteile auch im Fernunterricht via MS Teams gehalten oder in hybrider Form (Unterricht im Klassenzimmer mit Live-Übertragung per MS Teams) angeboten. Die gewählte Unterrichtsform orientiert sich dabei an den zu behandelnden Themen.

10 Kursbeschreibungen

Nachfolgend sind die einzelnen Kurse dieses Studienganges beschrieben.

Der Begriff Kurs schliesst alle Veranstaltungstypen ein, wie Vorlesung, Lehrveranstaltung, Fallstudie, Living Case, Fach, Studienreise, Semesterarbeiten usw.

10.1 Bedrohungen und Operational Security

Allgemein	In diesem Einführungsblock wird eine Übersicht über die aktuelle Bedrohungslage vermittelt. Im Weiteren werden die grundlegenden Arbeitstechniken behandelt und gezeigt, wie sich die Studierenden selbst und ihren Arbeitsplatz schützen, um bei ihrer Arbeit das Risiko möglichst tief zu halten. Grundlegende, für dieses CAS wichtige Basiskenntnisse werden mit einem kurzen Überblick und einigen Kontrollfragen zusammengefasst.
Lernziele	In diesem einleitenden Teil werden folgende Ziele angestrebt: – Die Studierenden sind über den weiteren Verlauf des CAS informiert. – Allfällige Lücken gegenüber den Voraussetzungen für das Studium im CAS sind erkannt und können selbstständig durch die Studierenden geschlossen werden. – Die Studierenden kennen die möglichen Sicherheitsbedrohungen und können sie richtig einordnen/typisieren. – Die Studierenden kennen den richtigen Umgang mit gefährlichem Material und wissen, wie sie sich und ihre Mitarbeiter*innen effektiv schützen können (Operational Security).
Themen und Inhalte	**Einführung und Bedrohungslage:** – Bedrohungen durch Cybercrime und staatlich geführte Cyberangriffe – Überlegungen zur Ethik – Schutz der eigenen Identität, Umgang mit Social Networks – Schutz der eigenen Arbeitsmittel (Anonymisierung, verschlüsselte Kanäle) und der Mitarbeitenden **Typisierung der Bedrohungen:** – Malware-Techniken – Akteure und ihre Werkzeuge **Typisierung von Malware:** – Trojaner – Würmer – Backdoors – Rootkits

Vorkenntnisse	Um optimal vom Studium im CAS profitieren zu können, sind folgende Vorkenntnisse erforderlich:
	– **Grundlagenwissen des SW-Development:**
	  – Perl, Python, PHP oder eine andere Skriptsprache
	  – Grundlagen der Programmierung in einer Shell
	  – Vertrautheit mit regulären Ausdrücken RegEx

Vorkenntnisse	– **Grundlagenwissen TCP/IP:**
	  – Online-Aufzeichnen und (offline) Analysieren von Datenströmen, mit Spezialisierung HW und SW auf Interlinks oder zwischen Server und Core-Netz
	  – Sniffing und Protokoll-Analyzer, Eigenschaften und Grenzen
	  – Filtermöglichkeiten, Filterregeln und HW-Filter, SW-Filter, Display-Filter
	  – Statistiken, Auswertungen und Aussagen
	  – Protokollanalyse
	– **Grundlagenwissen Betriebssystem-Theorie:**
	  – Aufbau eines Betriebssystems
	  – Prozessmanagement
	  – Memory Management
	  – Inter Process Communication
	  – Interrupts und die Kommunikation mit der Peripherie
	
	Der Umfang der Kenntnisse wird während der Einführung genauer erläutert. Es wird erwartet, dass die Studierenden dieses Wissen für das CAS dann selbstständig auffrischen resp. erarbeiten.

Lehrmittel	– Skript / kommentiertes Folienset – Training-Videos: https://www.wireshark.org/docs/ – Literaturempfehlungen Nr. 1, 2, 3

10.2 Prävention

Allgemein	Nur minimal oder schlecht geschützte Infrastrukturen sind unabhängig von den darauf verarbeiteten Daten ein lohnendes Ziel für Missbrauch. Systeme sind daher gegen direkte und indirekte Angriffe zu schützen, sprich zu härten. Die Effektivität der Massnahmen kann beispielsweise mittels Penetration Testing auf verschiedenen Ebenen geprüft werden. Aber auch gehärtete Systeme sind nie perfekt geschützt und neu gewonnene Erkenntnisse müssen ständig in die implementierten Sicherheitsmassnahmen einfliessen.
Lernziele	**Vulnerability- und Patch Management:** – Die Studierenden kennen die verschiedenen Arten von Schwachstellen, deren Einordnung und die entsprechenden Massnahmen zum Schutz von Infrastruktur und Systemen. – Die Studierenden wissen, wo sie Informationen zu Schwachstellen beschaffen können. Sie sind in der Lage, für das eigene Unternehmen zu beurteilen, in welchem Zeitraum ein Patch eingespielt werden muss. **Malware und Spam-Protection:** – Die Studierenden kennen die Möglichkeiten zum Schutz von Infrastruktur und Mitarbeitenden vor Malware und Spam. – Die Studierenden kennen die Malwareschutz-Strategie mit verschiedenen Schutzringen, welche die Grundlage für einen effizienten und effektiven Schutz legt. – Die Studierenden kennen die einzelnen Technologien, die den Schutz vor Malware und Spam ermöglichen.

Lernziele	**Cloud / System Hardening:** – Studierende können Serversysteme so aufbauen und konfigurieren, dass sie eine möglichst geringe Angriffsfläche bieten. Der Kurs ist zweigeteilt, der eine Teil behandelt das Hardening von Windows-Servern, der andere Teil das von Linux-Systemen. – Die Studierenden wissen, wie sie bei Cloud-Systemen und M365 im Speziellen die Sicherheit erhöhen können. **Penetration Testing:** – Die Studierenden können ihre Systeme und Anwendungen auf Verwundbarkeiten hin testen. – Die Studierenden wissen, mit welchen Arbeitsinstrumenten gearbeitet werden kann und kennen die nötigen Prozesse im Betrieb, um dies störungsfrei realisieren. – Die Studierenden kennen die Kategorisierung von webbasierten Sicherheitslücken nach OWASP Top Ten und wissen, wie diese Sicherheitslücken verhindert werden können.
Themen und Inhalte	**Vulnerability und Patch Management:** – Microsoft Windows vs. Unix – Klassifizierung von Schwachstellen – Informationsquellen – Issue- und Vulnerability-Tracking – Patch Cycles, Testing und zeitliche Aspekte – Grenzen des Vulnerability- und Patch-Managements **Malware und Spam Protection:** – Übersicht über die verschiedenen Möglichkeiten, sich vor Malware und Spam zu schützen – Malwareschutz: Strategien und Konzepte – Kenntnis über die Grenzen des Schutzes – Vom klassischen, signaturbasierten Scanner zu einem verteilten Ansatz mit verschiedenen Schutzelementen – Malware- und Virenscanner – Detektionsmöglichkeiten **Linux System Hardening:** – Generelles zu Unix-Konzepten und -Infrastrukturen – Unix Hardening Guides – Partitionierung und Diskchiffrierung – Härtung von Kernel und Netzwerkstack – Authentisierung und Autorisierung – Reduktion der Angriffsfläche durch Einschränken von Diensten – Mandatory Access Control am Beispiel von AppArmor – Integritätsprüfung – Sichere Remote-Administration mit SSH – Life Cycle Management – Logging

Themen und Inhalte	**Härtungsmassnahmen für Windows-Systeme:** – Generelles zu Microsoft-Konzepten und -Infrastrukturen – Windows Hardening Guides – Benutzerverwaltung und Authentisierung – Reduktion der Angriffsfläche durch Einschränken von Diensten – Microsoft Active Directory, Security Templates und GPOs – Tools zur Absicherung eines Windows Systems – Microsoft AppLocker – MS Best Practice Analyzer / Microsoft Baseline Security Analyzer – Lokale Firewall und Virenscanner – Microsoft BitLocker – Sichere Remote-Administration (RDP, etc.) – Logging **Cloud-spezifische Härtungsmassnahmen** (Fokus auf M365-Umgebungen): – Ausschalten von Legacy-Protokollen – Multifaktor-Authentisierung (Pro/Contra von verschiedenen Faktoren) – Schutz von hochprivilegierten Accounts – Deaktivieren vom Registrieren von Applikationen – Kennenlernen von Conditional Access Policies – Security Defaults – Handling von externen Benutzer*innen **Penetration Testing:** – Einordnung der Tests anhand der OSI-Layer 2–7 und Übersicht über die Tools (Portscanner, Vulnerability Scanner, Web Application Scanner, unterstützende Hilfsmittel) – Penetration Testing Standards (PTES, OSSTMM, OWASP, etc.) – Vorbereitende Vorsichtsmassnahmen und Massnahmen für den Fall, dass etwas schief geht – Portscanning (nmap, etc.) – Vulnerability Scanning (nessus, etc.) – Einsatz von Penetration Testing Frameworks (Metasploit & Co.) – Webapplication Scanning und manuelle Tests mittels Reverse Proxies. – Reporting – Was will ich? / Was erhalte ich? / Was mache ich daraus? – Grenzen des Penetration Testings – OWASP Top Ten Sicherheitslücken finden und beheben (Workshop)
Lehrmittel	– Skript / kommentiertes Folienset – Literaturempfehlungen Nr. 4, 5, 7

10.3 Detektion

Allgemein	Zu oft werden Angriffe erst nach Wochen oder Monaten per Zufall entdeckt. Mit geeigneten Tools und Massnahmen lassen sich Angriffe auf das Netzwerk und die Systeme deutlich rascher erkennen. Im Idealfall können automatisierte und gezielte Angriffe bereits kurz nach der ersten Kontaktaufnahme detektiert und durch gezieltes Einschreiten früh genug und bevor Schaden entsteht unterbunden werden.
Lernziele	**Logfile-Analyse:** – Die Studierenden kennen die Konzepte einer zentralisierten Logsammlung. – Die Studierenden erkennen Angriffsmuster in Logdaten. – Die Studierenden kennen Tools auf der Command Line für das effiziente Suchen in Logdaten und können sie anwenden. – Die Studierenden kennen ein SIEM-Tool und können einerseits darin strukturiert Daten sammeln und diese Daten andererseits auch auswerten. **Network Intrusion Detection Systeme (NIDS):** – Die Studierenden kennen die verschiedenen Konzepte für die netzwerkbasierte Intrusion Detection. – Die Studierenden erkennen Angriffsmustern auf Netzwerkebene. – Die Studierenden können ein Network Intrusion Detection System (NIDS) selbst aufbauen, parametrieren und einsetzen. **Host Intrusion Detection Systeme (HIDS):** – Die Studierenden kennen die Komponenten eines Host Intrusion Detection Systems (HIDS). – Die Studierenden kennen verschiedene Methoden der hostbasierten Intrusion Detection (Integritätsprüfung und Verhaltenserkennung) und kennen deren Vor- und Nachteile. – Die Studierenden lernen ein Host Intrusion Prevention Systems für Endgeräte kennen. **Cloud Monitoring:** – Die Studierenden kennen die spezifischen Herausforderungen der Überwachung von Cloud-Umgebungen, insbesondere bei hybriden Setups. – Die Studierenden kennen einige zentrale Tools für das Überwachen von Cloud-Umgebungen, wie z.B. Azure Sentinel. – Die Studierenden kennen verschiedene Log-Sourcen, die für die Aufarbeitung in einem Security Incident in der Cloud wichtig sind. **Dynamische Malwareanalyse:** – Die Studierenden kennen den Unterschied zwischen statischer und dynamischer Malwareanalyse. – Die Studierenden wissen, wie man mehr Infos zu einem Malwaresample dank OSINT-Informationen bekommt. – Die Studierenden können Sandboxberichte analysieren und auswerten.
Themen und Inhalte	**Logfile-Analyse:** – Zentralisierung von Logs mit Hilfe von Syslog – Logfile-Analyse auf der Kommandozeile – Pattern Matching

Themen und Inhalte	– Korrelationen
	– Einsatz von Splunk zur Logfile-Analyse
	
	Network Intrusion Detection Systeme (NIDS):
	– NIDS-Typen
	– Architektur eines NIDS
	– Konfiguration von Suricata
	– Verstehen von Suricata Rules
	– Analyse von pcaps und Generieren von IDS Rules
	– Praktische Übung
	– Zusätzliche Elemente wie passiveDNS
	
	Host Intrusion Detection Systeme (HIDS):
	– Konzept der hostbasierten Intrusion Detection
	– Elemente einer hostbasierten Intrusion Detection auf Server-Systemen
	– Integrity Checking Systeme als einzige Möglichkeit, die Unversehrtheit eines Systems nachzuweisen
	– Hostbasierte Analyse und Erkennung am Beispiel von OSSEC
	– Verhaltensbasierte Intrusion Detection auf Endgeräten mit Hilfe eines HIPS (Host Intrusion Prevention System)
	
	Cloud Monitoring:
	– Kennenlernen vom AWS Cloud Trail Log und die wichtigsten Elemente daraus
	– Ein grösserer Fokus wird auf das Monitoring und Erkennen von Kompromittierungen von M365-Umgebungen gelegt:
	  – Risky Sign-Ins
	  – Risk Detections
	  – Kennenlernen der verschiedenen Log-Files
	  – Gezieltes Hunting nach Kompromittierungen von EntraID Accounts
	
	Dynamische Malware Analyse:
	  – Statische/dynamische Malwareanalyse mit verschiedenen Tools.
	  – OSINT Informationen sammeln und richtig anwenden.
	  – Malwareanalyse in verschiedenen Sandboxes (Public/Private) und Auswertung der Reports.

Lehrmittel	– Skript / kommentiertes Folienset – Literaturempfehlungen Nr. 6, 8

10.4 Workshop

Allgemein	Workshop mit CSIRT des BIT.
Lernziele	Die Studierenden erhalten anhand von kleinen Aufgaben die Möglichkeit, den gelernten Stoff anzuwenden. Sie werden dabei anhand eines Fragebogens durch die verschiedenen Teilaufgaben geführt.
Themen und Inhalte	– Basiswissen Linux – Basiswissen Windows – Netzwerk-Sniffing

	– Mail Clients und deren Artefakte – Passwort Cracken – Schwachstellen – Untersuchungen von Binaries
Lehrmittel	– Die im Kurs abgegebenen Skripte – Ein «Spickzettel» für die wichtigsten Tools – Live-System / VMware Image mit der Testumgebung – «Google is your Friend»

10.5 Projektarbeit

Allgemein	Die Projektarbeiten sind Einzel- oder Gruppen-Arbeiten aus dem Arbeitsumfeld der Studierenden. Gruppenarbeiten sind wo immer möglich erwünscht und je nach Rahmenbedingungen meist von Vorteil. Der nominelle Aufwand liegt bei 90 Arbeitsstunden pro Gruppenmitglied, kann je nach Vorbereitungsphase und Komplexität der Aufgabenstellung aber auch leicht höher sein. Falls aus Sicht der Auftraggeber*innen notwendig, können die Ergebnisse der Semesterarbeiten vertraulich behandelt werden. Massgebend für die Rahmenbedingungen ist das Studienreglement. Die Vertraulichkeit darf den didaktischen Rahmen nicht behindern: Präsentationen und Diskussionen über das gewählte Thema müssen im Rahmen der Klasse möglich sein.
Zielsetzung und Thema	In der Semesterarbeit befassen sich die Teilnehmenden mit einem Projekt (ev. Teilprojekt) oder einer Fragestellung aus ihrer Firma. Mit dem gewählten Thema vertiefen die Studierenden die im Studium erlernten Methoden und wenden diese an einer konkreten Fragestellung in der Praxis an. Themen von Semesterarbeiten können beispielsweise sein: – Erarbeiten der zusätzlich notwendigen Massnahmen nach einem sicherheitsrelevanten Vorfall im eigenen oder einem auftraggebenden Betrieb – Untersuchung und Nachstellung neuer Angriffsmethoden – Analyse vorhandener Infrastruktur und anhand der gewonnenen Informationen ein geeignetes Konzept zur Härtung der Systeme erarbeiten – IoT-Security mit Vulnerability Assessment für Industrie-4.0-Anlagen – Sicherheits-Vorfälle oder -Projekte der Dozierenden
Ablauf	Die Semesterarbeit umfasst ca. 90h Arbeitsleistung pro Student*in und beinhaltet die folgenden Meilensteine (siehe auch Zeitplan): 1. In der Firma ein Thema suchen und finden sowie eine*n Ansprechpartner*in/Betreuer*in in der Firma definieren. 2. Erstellen einer Projektskizze (Wordvorlage vorhanden). 3. Die Projektskizze umfasst eine ein- bis maximal zweiseitige Aufgabenstellung mit folgenden Elementen: 1. Titel 2. Umfeld 3. Problemstellung

Ablauf	4. Lösungsansatz (Vorgehen, Methoden) 5. Angestrebte Ergebnisse und Ziele 6. Name und Kontaktadressen aller Gruppenmitglieder, und der Ansprechspartner*innen/Betreuer*innen der Firma 4. Individuelle Kurzpräsentation (10') und Diskussion (10') des gewählten Themas an der Schule vor einem Expert*innen- und Dozierenden-Gremium. 5. Eventuelle Ergänzung oder Überarbeitung der Projektskizze gemäss Feedback an der Präsentation. 6. Zuordnung eine/s/r Expert*in durch die Schule für die Begleitung der Semesterarbeit. 7. Durchführung der Arbeit mit eigener Terminplanung. 8. Ca. 2–3 Meetings mit dem Experten. – Projektskizze besprechen / Kick-off. – bei Bedarf: Zwischenreview / Beratung. – Schlusspräsentation vor dem Expert*innen- und Dozierenden-Gremium. – Dauer: 10'–15' und Diskussion: 10'–15' pro Arbeit. 9. Abgabe des Berichtes auf der Studienplattform oder nach Absprache per E-Mail an den/die Expert*in. 10. Beurteilung durch den/die Expert*in.
Ergebnis und Bewertung	Der Bericht ist in elektronischer Form, als PDF-Dokument dem/der bewertenden Expert*in und der CAS-Leitung über die Studienplattform (aktuell Moodle) abzugeben. Der Bericht umfasst ca. 20 Seiten. Der Source Code ist, soweit für die Projektbeurteilung notwendig, als Anhang mitzuliefern. Die Semesterarbeit wird nach den folgenden Kriterien bewertet: – Themeneingabe Projektskizze rechtzeitig und vollständig eingereicht. Themenpräsentation sorgfältig vorbereitet. Idee oder Aufgabe durchdacht und abgegrenzt, Quellen recherchiert, Rahmenbedingungen definiert, Teilziele priorisiert. – Methodik und Ausführung Gewählte Methode(n) systematisch und korrekt angewendet. Kreativ und agil in der Ausführung. Entscheidungen präzis begründet. – Ergebnis Nachvollziehbares und dokumentiertes Ergebnis. Aufgabenstellung erfüllt. Ergebnisse validiert, getestet, verifiziert. Vergleich von Zielsetzung und Ergebnis vorgenommen. Learnings und Ausblick vorhanden. – Bericht und Dokumentation Vollständig und verständlich. Rechtschreibung korrekt. Kapiteleinteilung sinnvoll. Angemessene Darstellung. Grafiken auf das Wesentliche reduziert und beschriftet. – Schlusspräsentation Roter Faden, logisches Vorgehen, klare Aussagen. Identifikation mit dem Thema spür- und erkennbar. Professionelle Präsentationstechnik,

	Zeitvorgaben genutzt und eingehalten. Fragen präzis und sicher beantwortet. Die aufgeführten Kriterien sind durch die Expert*innen entsprechend dem bearbeiteten Thema und dem Ablauf der Arbeit in ihrem Gewicht anpassbar.

11 Kompetenznachweis

Für die Anrechnung der 12 ECTS-Credits ist das erfolgreiche Bestehen der Qualifikationsnachweise (Prüfungen, Projektarbeiten) erforderlich, gemäss folgender Aufstellung:

Kompetenznachweis	Gewicht	Art der Qualifikation	Erfolgsquote Studierende
Bedrohung und Operational Security		keine	
Prävention	3	Gruppenarbeit / Prüfung	0 – 100 %
Detektion	2	Gruppenarbeit / Prüfung	0 – 100 %
Workshop mit CSIRT BIT	1	Gruppenarbeit (Workbook)	0 – 100 %
Fallstudie/Semesterarbeit	4	Bewertete Projektarbeit	0 - 100 %
Gesamtgewicht/Erfolgsquote	**10**		0 – 100 %

Der gewichtete Mittelwert der Erfolgsquoten der einzelnen Kompetenznachweise wird in eine Note zwischen 3 und 6 umgerechnet. Die Note 3 (gemittelte Erfolgsquote weniger als 50%) ist ungenügend. Die Noten 4, 4.5, 5, 5.5 und 6 (gemittelte Erfolgsquote zwischen 50% und 100%) sind genügend.

12 Lehrmittel

Sollten gemäss Kapitel 4 (Voraussetzungen) Wissenslücken bestehen, werden zur Vorbereitung folgende Lehrmittel empfohlen:

Nr.	Titel	Autoren	Verlag	Jahr	ISBN-Nr.
1	LINUX - Das umfassende Handbuch	Michael Kofler	Rheinwerk Computing	2023	978-3-8362-9620-5 (auch als e-Book)
2	RegexOne, Learn Regular Expressions with simple, interactive exercises.	RegexOne	Internet	2023	Link
3	Computernetzwerke 6. Auflage (Deutsche Übersetzung)	Andrew S. Tanenbaum Nick Feamster David J. Wetherall	Pearson Studium	2024	978-3-86894-452-5

Ergänzende Lehrmittel sind Empfehlungen, um den Stoff zu vertiefen oder zu erweitern. Die Beschaffung liegt im Ermessen der Studierenden:

Nr.	Titel	Autoren	Verlag	Jahr	ISBN-Nr.
4	Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code	Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard	John Wiley & Sons, Ltd.	2014	978-0470613030
5	Learn Penetration Testing	Pillay Rishalin Pillay	Packt Publishing	2019	978-1-83864-416-1
6	The Cybersecurity Playbook for Modern Enterprises	Jeremy Wittkop	Packt Publishing	2022	978-1-80324-863-9
7	Penetration Testing Azure for Ethical Hackers	David Okeyode Karl Fosaaen	Packt Publishing	2021	978-1-83921-293-2
8	Microsoft Azure Security Technologies Certification and Beyond	David Okeyode	Packt Publishing	2021	978-1-80056-265-3

13 Dozierende

Vorname Name	Firma	E-Mail
Endre Bangerter	Berner Fachhochschule	endre.bangerter@bfh.ch
Stephan Berger	Infoguard	stephan.berger@bfh.ch
Eduard Blenkers	BLS	eduard.blenkers@bfh.ch
Stefan Egger	Bundesamt für Informatik und Telekommunikation	stefan.egger@bfh.ch
Marco Gfeller	Bundesamt für Cyber Sicherheit	marco.gfeller@bfh.ch
Reto Inversini	SBB	reto.inversini@bfh.ch
Heino Kronenberg	Bundesamt für Informatik und Telekommunikation	heino.kronenberg@bfh.ch
Dominik Kuhn	Bundesamt für Informatik und Telekommunikation	dominik.kuhn@bfh.ch
Adrian Leuenberger	VBS	adrian.leuenberger@bfh.ch
Manuel Schilt	VBS	manuel.schilt@bfh.ch
Mauro Vignati	ICRC	mauro.vignati@bfh.ch

14 Organisation

CAS-Leitung:
Dominik Kuhn
E-Mail: dominik.kuhn@bfh.ch

CAS-Administration:
Miriam Patwa
Tel: +41 31 848 58 68
E-Mail: miriam.patwa@bfh.ch

Während der Durchführung des CAS können sich Anpassungen bezüglich Inhalten, Lernzielen, Dozierenden und Kompetenznachweisen ergeben. Es liegt in der Kompetenz der Dozierenden und der Studienleitung, aufgrund der aktuellen Entwicklungen in einem Fachgebiet, der konkreten Vorkenntnisse und Interessenslage der Teilnehmenden, sowie aus didaktischen und organisatorischen Gründen Anpassungen im Ablauf eines CAS vorzunehmen.

Berner Fachhochschule
Technik und Informatik
Weiterbildung
Aarbergstrasse 46
2503 Biel

Telefon +41 31 848 31 11
E-Mail: weiterbildung.ti@bfh.ch

bfh.ch/weiterbildung
bfh.ch/cas-sipd

Berner
Fachhochschule