Short Advanced Studies (SAS)[1]

Cyber Threat Intelligence – Specialist 1

Gain hands-on experience with industry tools and techniques. Learn how to collect, analyze, and pivot intelligence using real-world platforms and frameworks used by CTI professionals.

[1]Short Advanced Studies (SAS) are short qualifying training courses designed for a specialist audience seeking to face new challenges in direct dialogue with experts (1-9 ECTS).

Berner
Fachhochschule

Table of Contents

16. Sep. 2025

1 Portrait

CTI Specialist I is a practical, hands-on module focused on the tools, methodologies, and workflows used by cyber threat intelligence analysts in real-world environments.

Participants will work with primary data sources such as malware samples, IP addresses, domains, certificates, and code reuse indicators. The module emphasizes the importance of structured analytical approaches, including frameworks such as MITRE ATT&CK, the Diamond Model, and DISARM.

A central component of the course is mastering widely used CTI tools and platforms, including Maltego, OpenCTI, VirusTotal, MISP, Shodan, and others. Students will learn how to extract, correlate, and enrich data to generate meaningful intelligence.

The module also introduces key techniques such as pivoting on indicators of compromise (IoCs), applying OSINT methodologies, and understanding adversary tactics, techniques, and procedures (TTPs).

Through case-based exercises and practical labs, participants develop the ability to track threat actors, analyze incidents, and produce actionable insights.

This module equips students with the technical skills required to operate effectively as a CTI analyst in professional environments.

2 Career opportunities

The SAS CTI-Specialist 1 program will prepare students for career opportunities in a variety of organizations:

- Law enforcement (police intelligence) – Federal agencies, KAPOs
- Military and government intelligence – CERTs, cyber-troops
- Finance industry – cyber fraud intelligence teams
- Large enterprises – IT/Cyber security and CTI teams
- Consultancy firms with a focus on cyber security
- IT/Cyber intelligence providers and product vendors
- Private boutique (specialized) intelligence firms

3 Target audience

The SAS CTI-Specialist 1 is designed for IT and Cybersecurity professionals wanting to specialize in cyber threat intelligence, working in the role of CTI analyst.

4 Education goals

This continuing education program has practical learning objectives. Students completing the SAS CTI-Specialist 1 will understand the concepts of cyber threat intelligence, and have skills for intelligence gathering, analysis, and dissemination. The program will focus on the use of industry-level capabilities, like threat intelligence analysis tools and platform for information sharing. Students will understand how to operationalize their work for a variety of customers and end-users.

5 Requirements

Admission into the SAS CTI-Specialist 1 requires one of the following:

- A university degree or equivalent professional education degree in computer science, computer engineering, cyber security, or related field
- Professional experience in cyber security, threat intelligence, digital forensics or IT investigation, and a related industry certification

If applicant qualifications are unclear or inconclusive, further information (for example a CV) or an interview may be requested.

6 Factsheet

Short Advanced Studies (SAS)	Cyber Threat Intelligence – Specialist 1
Degree/Certificate	Short Advanced Studies (SAS)
Duration	One week, 5 days
Application deadline	Up to 1 month before the start of the course
ECTS credits	3
Costs	CHF 2'500
Teaching language	English
Location	BFH-TI at Switzerland Innovation Park in Biel/Bienne

7 Content + Learning objectives

Educational objectives	This first specialist module will focus on a hands-on course on the tooling set a threat intel analyst is usually using in the industry and how to apply techniques gain intelligence.
Topics and content	– Primary collection sources and collections sources (malware, IP/Domains, TLS certs, code reuse, etc.). – Mastering the kill chain: MITRE ATT&CK, DISARM, and Diamond Model – Mastering the Tools: Maltego, OpenCTI, VirusTotal, MISP, Shodan, Certstream, Zonefiles, CyberChef, Yara, Yara-X, Sigma, etc. – Understnading pivoting IoCs, OSINT methodologies, adversary TTPS. – InfoOps: tracking actors, dissecting cases, applying DISARM.
Course material	Provided in Moodle

8 Proof of proficiency

To receive 3 ECTS (European Credit Transfer and Accumulation System) academic credits, students must demonstrate their knowledge by successfully completing assignments, projects, and final exam as required by the lecturer. Students who attend all classes but do not complete the assessment work will receive a certificate of attendance equivalent to 40 CPE (Continuing Professional Education) hours.

9 Lecturer

Name	Organisation	E-mail
Konstantin Klinger	Lecturer BFH	konstantin.klinger@bfh.ch

10 Organisation

SAS supervisor:
Mauro Vignati
Phone: +41 79 617 72 64
E-mail: mauro.vignati@bfh.ch

SAS administration:
Miriam Patwa
Phone: +41 31 848 58 68
E-mail: miriam.patwa@bfh.ch

Note: Changes may be made to content, learning objectives, lecturers and required proficiency levels. The lecturers and the Head of Studies are authorized to make adjustments to a SAS on the basis of current developments in a subject area, the specific previous knowledge and interests of the students, or for didactic and organizational reasons.

Bern University of Applied Sciences
School of Engineering and Computer Science
Continuing Education
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel/Bienne

Phone +41 31 848 31 11
E-mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/weiterbildung