Short Advanced Studies (SAS)[1]

Cyber Threat Intelligence – Specialist 2

Advance your CTI capabilities with deep web investigations, blockchain analysis, and threat hunting. Explore how intelligence supports detection, risk management, and cyber defense strategies.

[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

Organizations today operate a complex interconnected landscape of traditional IT, IoT, and OT infrastructure to provide communication, access to resources, and interaction with the physical world. Employees are in the office, on the road, and working from home. They use office desktops, VDIs, mobile devices, and personal (BYOD) equipment. IT and information assets are on-premises, in the cloud, and out-sourced to third parties. IoT and OT devices are expanding the traditional IT landscape to include smart buildings and environments, and various Internet enabled gadgets.

This infrastructure is under constant threat of cyber-attack, both targeted and opportunistic. Cyber Threat Intelligence (CTI) helps protect organizations by gathering, analysing, and disseminating information about threat actors, new vulnerabilities, and increasing risks to this infrastructure.
The SAS CTI Specialist 2 course prepares you specifically for an exciting career in a future CTI role as a Cyber Threat Intelligence Analyst.

2 Career opportunities

The SAS CTI-Specialist 2 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 2 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 2 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 2 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 2
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 second specialist module will focus on secondary collection sources, and on the various aspects of CTI, from vulnerability management to threat hunting.
Topics and content	– Secondary collection sources: intelligence feeds providers, cyber security partners, ISPs, certificates and open-source collection – Fundamentals on blockchain (cryptocurrencies, DeFi, tumblers, bridges, etc.). – Deep- and Dark web monitoring and investigations. – On-Chain crime: investigation, crypto laundering. Mastering the tools like Etherscan, Chainabuse, OXT, MistTrack, etc. – CTI and: Threat Hunting/detection engineering; Vulnerability Management/Attack Surface Reduction; Brand protection/VIP protection; Risk Management; Cyber Fraud; Tabletop Excercies and Best Practices
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
Mauro Viganati	Lecturer BFH	mauro.vignati@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