Short Advanced Studies (SAS)[1]

Cyber Threat Intelligence Advanced

Deepen your CTI expertise by analyzing adversaries, mastering intelligence reporting, and exploring advanced topics such as attribution, AI, and secure communication technologies.

[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

29 Jan. 26

1 Portrait

The CTI Advanced module expands on foundational knowledge by focusing on the behavior, capabilities, and structure of cyber adversaries, as well as advanced analytical practices.

Participants will examine different threat actor categories, including state-sponsored groups, cybercriminal organizations, and hacktivists. The module explores how to cluster and analyze these actors based on their tools, techniques, intent, and operational patterns.

A key component of the course is intelligence communication. Students learn how to structure, write, and disseminate high-quality intelligence reports, as well as how to share information effectively using established protocols.

The module also introduces the concept of attribution and its challenges, along with advanced topics such as anonymity in network traffic, cryptography, and the role of emerging technologies like artificial intelligence and machine learning in both offensive and defensive contexts.

By combining analytical rigor with practical communication skills, this module prepares participants to produce actionable intelligence and support decision-making at strategic and operational levels.

2 Career opportunities

The SAS CTI-Advanced 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-Advanced 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 Advanced understand the concepts of cyber threat intelligence and have knowledge of information 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-Advanced 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 Advanced
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 module will look at several advanced aspects, like adversaries tooling, capabilities, intent and structure, but also to some advanced threat intelligence skills, like analysis and reporting, information sharing, and an introduction to the toolsets.
Topics and content	– Adversaries: who's who, capabilities, tooling, presence, intent, structure. From state-sponsored to semi-state sponsored, to cybercrime actors and hacktivists. Clustering groups and operations. – Threat intelligence sharing, dissemination: from protocols for sharing to how to write an analysis. – Attribution – Traffic anonymity, AI (ML, language models, prompt hacking), cryptography and cloud technologies.
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
Emilia Cebrat-Maslowski	Director of Threat Intelligence at Quad9, Product Owner for Cyber Threat Intelligence at Switch

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