Short Advanced Studies (SAS)[1]

Cyber Threat Intelligence – Fundamentals

Build the essential foundations of Cyber Threat Intelligence. Learn how to understand threats, structure intelligence processes, and translate complex cyber risks into actionable insights for organizations.

[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

28 May 2026

1 Portrait

The CTI Fundamentals module introduces the core principles of Cyber Threat Intelligence and provides a structured understanding of how intelligence supports cybersecurity operations. Participants explore key concepts such as intelligence terminology, the intelligence cycle, and analytical techniques used to assess threats and risks. The course also covers threat modelling approaches and widely used frameworks, enabling students to better understand adversaries and their potential impact.

A strong emphasis is placed on distinguishing between data-driven and concept-driven analysis, as well as defining intelligence requirements and priorities. Students will also gain insight into how CTI functions within different organizational contexts—from corporate security operations to government use cases.

In addition, the module introduces the technical and organizational environment in which CTI operates. This includes an overview of SecOps concepts such as SIEM and SOAR, as well as the structure of modern IT ecosystems (cloud, on-premises, and supply chains).
By the end of this module, participants will have a solid foundation to understand, contextualize, and communicate cyber threats effectively.

2 Career opportunities

The SAS CTI-Fundamentals 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-Fundamentals 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 Fundamentals understand the concepts of cyber threat intelligence and have knowledge of information gathering, analysis and dissemination. Students recognize how they can operationalize their work for a variety of clients and end users.

5 Requirements

Admission into the SAS CTI-Fundamentals 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 Fundamentals
Degree/Certificate	Short Advanced Studies (SAS) in Cyber Threat Intelligence Fundamentals
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 SAS teaches the fundamentals of Cyber Threat Intelligence
Topics and content	– Understanding intelligence and cyber threat intelligence: lexicon, terminology, intelligence cycle, analytical techniques. Defining threats and understanding risks – Threat modelling and threat frameworks – Data-driven vs. conceptually driven analysis, intelligence gathering vs. consumption, CTI requirements and priority intelligence requirements – The CTI business, defining scope and purposes: CTI for cyber security, CTI as information advantage, CTI as core business, CTI for government. Building a threat intel team. – Company environment: introduction to SecOps (SIEM, SOAR, etc.), understanding corporate network and environment. Understanding a standard technology stack, weakness and strengths (supply chain security, SaaS vs on.prem, etc.).
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
Lorenzo Pagnamenta	Head of Threat Intelligence, ABB

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

Berner
Fachhochschule