

## Project: Configuration and Application of SIEM Systems

Course Code: DLBCSEEISC02\_E

Study Level	Language of Instruction and Examination	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEEISC01_E or DLBCSEEISC01_D

### Course Description

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats. Furthermore, students will face the challenge to transfer technical data into operational Information to initiate valid responses. By the end of this course, students will have obtained well-founded knowledge of the integration of SIEM into enterprise IT infrastructure, applications and services.

### Course Outcomes

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

### Contents

- This course focuses on practical aspects of the implementation of a SIEM into an enterprise IT infrastructure environment. Students start with a chosen use case and SIEM and then evaluate requirements which need to be fulfilled so that the SIEM can be used as part of an enterprise IT system / network. Students need to evaluate requirements for sensors, network monitoring, intrusion detection, data fusion, big data analytics, and translating technical data into operational information.
- Based on the available information, valid responses – including automated responses - will be identified and processed.
- All relevant artifacts and considerations are documented by the students in a project report.

**Literature****Compulsory Reading****Further Reading**

- Al-Sakib, K. P. (2016): The State of the Art in Intrusion Prevention and Detection. Routledge, Abingdon.
- Miller, D. et al (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY.
- Mitchell, H. B. (2007): Multi-Sensor Data Fusion: An Introduction. Springer Verlag, Berlin.

**Study Format Fernstudium**

<b>Study Format</b> Fernstudium	<b>Course Type</b> Project
------------------------------------	-------------------------------

Information about the examination	
<b>Examination Admission Requirements</b>	<b>BOLK:</b> no <b>Course Evaluation:</b> no
<b>Type of Exam</b>	Written Assessment: Project Report

Student Workload					
<b>Self Study</b> 120 h	<b>Contact Hours</b> 0 h	<b>Tutorial</b> 30 h	<b>Self Test</b> 0 h	<b>Independent Study</b> 0 h	<b>Hours Total</b> 150 h

Instructional Methods	
<input type="checkbox"/> Learning Sprints® <input type="checkbox"/> Course Book <input type="checkbox"/> Vodcast <input type="checkbox"/> Shortcast <input type="checkbox"/> Audio <input type="checkbox"/> Exam Template	<input type="checkbox"/> Review Book <input type="checkbox"/> Creative Lab <input checked="" type="checkbox"/> Guideline <input type="checkbox"/> Live Tutorium/Course Feed <input checked="" type="checkbox"/> Slides