**8** DLBCSEEISC02\_E

Project: Configuration and Application of SIEM Systems

**Course Description**

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) tool in 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 of converting technical data into operational information to initiate valid responses. By the end of this course, students will have obtained a sound understanding of the integration of SIEM into enterprise IT infrastructure, applications and services.

**Contents**

▪ This course focuses on practical aspects of the implementation of a SIEM tool into an enterprise

IT infrastructure environment. Students start with a chosen use case and SIEM tool and then evaluate the requirements that need to be fulfilled so that 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 will be documented by the students in a project report.