## description: Valgfrit modul VF4 SIEM og log-analyse (5 ECTS)

# Lecture planning

## Course title: VF4 SIEM og log-analyse (5 ECTS)

English: SIEM and Log Analysis

Teacher: Henrik Kramselund xhek@kea.dk +45 2026 6000

This document is written in markdown, uploadet to GitHub.

The link for this is:
https://github.com/kramse/kea-it-sikkerhed/tree/master/siem-og-loganalyse

### Goals

The module is centered around Security information and event management (SIEM) and log analysis including common SIEM systems, logging, gathering, processing and working with logs.

Teaching material will primarily be English, but the teaching will be in Danish.

See more about the course in the official curriculum which can be downloaded from the main page
https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed

- near the top "Download studieordningen".

### Dates:

- Lecture lessons
- Group exercises and cases, including practical exercises with laptop

Teaching dates: tuesdays and thursdays 17:00 - 20:30

Teaching dates: mostly tuesdays and thursdays 17:00 - 20:30
29/10 , 31/10 - moving to new date! , 5/11 , 7/11 , 12/11 , 14/11, 19/11

Suggestion for replacement date 26/11

Exam: 2/12 2024

Make sure to mark dates in your calendar

### Hardware

Since we are going to be doing exercises, each team will need virtual machines.

The following are recommended:

- One based on Debian 12, running software servers and web applications

Read more about these at https://github.com/kramse/kramse-labs

# Course reading list

This course uses three books and a number of supporting resources.

Primary literature:

- Data-Driven Security: Analysis, Visualization and Dashboards
  Jay Jacobs, Bob Rudis
  ISBN: 978-1-118-79372-5 February 2014
  https://datadrivensecurity.info/ - short DDS

- Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan
  by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405 - short CIP

- Intelligence-Driven Incident Response
  Scott Roberts Rebekah Brown ISBN: 9781098120689 **2nd edition 2023** - short IDIR

- Modern Security Operations Center, The
  ISBN: 978-0135619858 Joseph Muniz - short SOC

It is recommended to buy these books.

Also the course will use internet links and pages. These can be downloaded from the internet often for free and may be gathered by the instructor for easy download.

Supporting literature:

- Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7 - shortened LBfH

This book introduces the Linux operating system commands, using Kali Linux as example. The tools presented include a lot of generic Unix tools. If you have no experience with Linux or Unix it is recommended to buy this book.

Installing and running the specific Linux distributions used is described in these books

- The Debian Administrator's Handbook, Raphaël Hertzog and Roland Mas
  https://debian-handbook.info/ - shortened DEB

- The Linux Command Line: A Complete Introduction, 2nd Edition, William Shotts
  Download -- internet edition https://sourceforge.net/projects/linuxcommand

- Kali Linux Revealed Mastering the Penetration Testing Distribution https://www.kali.org - shortened KLR

In the Network and Communications Security course we use this book:

- Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders ISBN: 9780124172081 -- I highly recommend this book

## Supporting Internet resources

Apart from the books a lot of blogs, papers and other resources are available. Often these can be downloaded from the internet.

- The JavaScript Object Notation (JSON) Data Interchange Format RFC8259
  https://tools.ietf.org/html/rfc8259

- Privacy by design in big data: An overview of privacy enhancing technologies in
  the era of big data analytics, ENISA

[https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport](https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport)

- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D.
  Lockheed Martin Corporation
  [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)

- The Diamond Model of Intrusion Analysis, Sergio Caltagirone, Andrew Pendergast, Christopher Betz
  [http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf](http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)

- Development of a virtualized security operations center, Robert de Céspedes, George Dimitoglou
  [https://dl.acm.org/doi/abs/10.5555/3512489.3512501](https://dl.acm.org/doi/abs/10.5555/3512489.3512501)

- Network Security Visualization, Keith Fligg and Genevieve Max

- Passive TCP Reconstruction and Forensic
  Analysis with tcpflow, Garfinkel, Simson L.; Shick, Michael,
  Monterey, California. Naval Postgraduate School, 2013-09-02

- Visualizing Network Activity using Parallel Coordinates,
  Sebastien Tricaud, Kara Nancem, Philippe Saadé

Other relevant papers and documents can often be found in the NIST publications, Special Publications series 800:
[https://csrc.nist.gov/publications/sp800](https://csrc.nist.gov/publications/sp800)

Example the Guide to Computer Security Log Management SP800-92

# Planning

The detailed plan is below with a table summarizing lessons.

**Note: might contain lot of pages, learn to skim and skip chapters and parts that don't interest you. In real life we don't have time to read every word!**

Also I have decided to include some papers in this course. Remember to check references in the books for supplementary reading.

Note about software: The books may describe installation of software, but those parts often become outdated so don't follow those to closely!

| Week | Theme / Goals | Litterature / Preparation |
|---|---|---|
| 29/10 | Welcome, goals and expectations<br><br>Prepare Virtual Machines - bring laptop<br><br>Create a good starting point for learning Introduce lecturer and students Concrete Expectations Prepare tools for the exercises | Reviewing the literature list will occur when we meet.<br><br>Download resources<br><br>Identification of chapters from books for reading as home assignment<br><br>Start lab setup and asses programming knowledge |

| Week | Theme / Goals | Litterature / Preparation |
|---|---|---|
| 5/11 | **Initial Overview of SIEM Terms**<br>Get an overview of the subject | Books: approx 61 pages without the skim part, lots of pictures<br><br>DDS 1. The Journey to Data-Driven Security 18<br><br>DDS 2. Building Your Analytics Toolbox: R and Python 17<br><br>CIP 1 Incident Response Fundamentals 13<br><br>CIP 2 What Are You Trying to Protect? 13<br><br>Skim CIP 3 What Are the Threats? 14 |
| 7/11 | **Hello world of Security Data Analysis**<br>Get started with some data types and sources | Books: about 61 pages, lots of pictures<br><br>DDS 3. Learning the "Hello World" of Security Data Analysis 31<br><br>DDS 4. Performing Exploratory Security Data Analysis 30<br><br>Do exercises if you feel like it, notice how small valuable programs can be |
| 12/11 | **Storing and Processing data** | Books: 23 pages, but also parts of CIP 7!<br><br>CIP 4 A Data-Centric Approach to Security Monitoring 23<br><br>Skim read: CIP 7 Tools of the Trade 57, need to know NetFlow, DNS, and HTTP proxy logs in the real-world<br><br>Skim read: DDS 8. Breaking Up with Your Relational Database 25 |
| 14/11 | **Visualization and Dashboards** | Books - approx 44 pages<br><br>DDS 6. Visualizing Security Data 22, DDS 10. Designing Effective Security Dashboards 22<br><br>Skim: DDS 11. Building Interactive Security Visualizations 26 |

| Week | Theme / Goals | Litterature / Preparation |
|---|---|---|
| 19/11 | **Baseline Your Data** | Books - approx 64 pages<br><br>DDS 7. Learning from Security Breaches VERIS 28<br><br>DDS 12. Moving Toward Data-Driven Security 11<br><br>IDIR 1. Introduction 8<br><br>IDIR 2. Basics of Intelligence 17 |
| 26/11 | **Operate, Respond and Forensics** | Books - approx 68 pages<br><br>SOC 7. vuln management 25, SOC 11. Reacting to events and Incidents 16, CIP 6 Operationalize! 27<br><br>Papers: Skim table of contents Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics, ENISA |

# Skipped chapters

We are reading mostly from the DDS book, but we are also skipping a few chapters.

We are skipping these:
DDS 5. From Maps to Regression 33 pages - skipped, as Elasticsearch provides the math we need.

DDS 9. Demystifying Machine Learning 25 pages - skipped, as this is complex subject in itself.

Note: a recent book was published about this subject: Machine Learning and Security
Clarence Chio ISBN: 9781491979907

We also skipped other chapters, which I would have liked to include:

- SOC 1. Introduction to Security Operations and the SOC 33 pages
- SOC 2. Overview of SOC Technologies 32 pages
- SOC 6. Security Event Generation and Collection 66 pages

I have tried to include important conclusions from those chapters in the slides.