Certificate

Basics and concepts of information security monitoring

User **Rene@Karkkainen.net** has completed **100%** of section **Basics and concepts of information security monitoring**.

100 %

Description:

In this course, we go through the concepts related to the organization's information security control.

Completed modules:

- What is information security monitoring?
- False positive vs false negative

- IDS/IPS systems
- What are security incidents? What should be collected and when should an alarm be raised?
- SIEM systems
- Adding a log source to the ELK Stack
- Examining logs exercise 1
- Examining logs exercise 2
- Examining logs exercise 3
- Alarms in data security monitoring