Exam subjects, with keywords

Key words will not be in the exam setting, only the subject title.

You are expected to prepare a 10min presentation in each subject. Then during exam you will draw one of the subjects and have 10min to go through this.

Make sure to relate it all to SIEM systems, log analysis and the overall picture

1) Overview of SIEM

The SIEM name, dive into events - common data used/found in events
SOC, IOC and other acronyms that are found in this course

Try to make an overview for someone new to the field

2) Data types

IP address, domain names and DNS, reputation lists, formats JSON, XML, CSV
ISO8601 - normalization
Netflow and TCP/IP, AS numbers, CIDR, port numbers

3) Tools used in the SIEM world

Languages, Zeek, Python, cURL, JavaScript, CSS, R
Any tools you like, really

4) Storing and processing data -- log data in particular

Elastic stack, Logstash - ingestion and normalization, Elasticsearch - store/process, Kibana present
REST, Message queuing
Filebeat, packetbeat

5) Dashboards and visualization of event data

process of using, searching in data
Elasticsearch Elastic Common Scheme (ECS) Elasticsearch SIEM
How standard schemes help

6) SIEM architectures

Present some sample architectures, use some of the tools presented like HELK and Elastic stack overviews

Explain some problems - scalability, how to cope with lots of data