Hand-in assignment I: KEA SIEM and Log Analysis course

Assignment:
Consider a system environment running the services we have presented in this course. The services are:

- Elasticsearch server, we ran this early in the course and this can be used for running a SIEM in production
- Kibana we have run this multiple times during the course
- Syslog server using Logstash – note we have talked very little about Logstash, so need to do a little *independent research*

Create a report describing the following in main chapters:

- Company back story, create back story for your fictive company, half a page
- Describe the software requirements for each of the above systems, copy paste the requirements from elastic home page perhaps
  Dont forget that these systems cannot float in free space, but requires one or more operating systems, which you must choose. Maybe include some monitoring and configuration management like Ansible.
- Describe the hardware requirements for your initial proof-of-concept deployment, taking into account creating a more production ready system. Do you need development, staging, testing, production systems, some redundancy or scalability?
- Suggest an initial deployment overview - little detail, with a naming scheme to use for servers, physical and virtual
  I would probably end up with about 10 servers for a small PoC
- Create a list of skills requirements for running this environment. Consider job postings for similar jobs, and you may copy parts of that and adapt

Note: you decide the versions to base this on.

The report should include the following sections at least:

- Title, Table of contents, formal report thanks
- Confidentiality agreement – Write ”Confidential” on each page
- Appendices

Must be handed in as PDF before exam.

Teams up to 3 are allowed. Make sure to list team members in the report.

Expect PDF as A4, portrait mode around 15 pages with illustrations as needed. No more than 25 pages if 3 members.

Hand-in assignment I: KEA SIEM and Log Analysis course

Recommend to use a report template with table of contents, front matter, page numbers etc. You can use Word, Google Docs, LaTeX, whatever you feel most comfortable with.

You are NOT expected to spend more than 25-30 hours on this. Less is also OK.

The report is not graded, but feedback will be given.

Help:
Consider this a proposal for your management team.

Think about what you would like to receive if you were responsible for buying hardware, selecting software and hiring people.

If you need more help contact me,

Henrik Kramselund Jereminsen, `xhek@kea.dk` `hlk@zencurity.dk`.