- **Security Monitoring 101**
  - Log Sources
  - Security monitoring protocols
  - Security monitor Infrastructures
  - Roles and responsibilities
  - Solutions in the market

- **RSyslog**
  - Syslog server deployment
  - Collecting logs from network devices
  - Collecting logs from Linux devices
  - Collecting logs from Windows devices

- **ELK Stack**
  - Architecture
  - Logstash deployment
    - Installation
    - Logs collection
    - Logs parsing
  - Elasticsearch
    - Installation
    - Index creation
    - Clusters
    - Connecting with Logstash
  - Kibana deployment
    - Installation
    - Connecting with Elasticsearch
    - Searching
    - Graphs & dashboard creation
  - Known problems and best practices

- **Graylog**
  - Architecture
  - Starting VM
  - System configuration
  - Adding Log Sources
  - Parsing logs
  - Searching
  - Alerts
  - Dashboards

- **Splunk**
  - Installation
  - System settings
  - Getting data into Splunk
  - Searches
  - Advanced searches
  - Dashboards and reports

- Datasets and Common Information Models
- Using Lookups
- Scheduled reports and Alerts
- Using Pivots

- **Security Onion**
  - Tools and Architecture
  - Standalone Installation
  - System configuration
  - Sguil Interface
  - ElasticSearch Interface
  - Deployment options

- **Open threat Intelligence Integration**
  - Open Threat Exchange
  - Vulnerability Feeds
  - Public black lists

- **Strategy for effective security monitoring**
  - What to monitor?
  - Data log retention policy
  - Security monitoring maturity levels