Assignment 5

Theme GDPR

Task 1
Aim: Gain main knowledge about GDPR and understand steps for this process
Read and explain how to provide GDPR compliance. Write a guide of GDPR process for your own project. Defend this task

Task 2
Aim: Gain theoretical and practical skills in working with SIEM

1) Read general information about SIEM.
2) Download http://www.splunk.com/ru_ru/download/splunk-enterprise.html
3) dpkg -i splunk_package_name.deb (for SETUP)
4) opt/splunk/bin/splunk start (to START)
5) Settings – Data Input - Files & directories
6) New → auth.log (var/log/.auth.log —---> continuously monitor
7) sourcetype – operating system —---> linux_audit —-> Start searching
8) ettings – Data Input - Files & directories —-> Add a home directory, create and delete several files in it, View the event log in Splunk
9) Settings – Data Input - Files & directories → Add a few more files, directories and logs
10) Search and Reporting → Find events var/log/.auth.log(source=var/log/.auth.log) Provide some operations like data filter, requests.
11) Download IDS Snort https://splunkbase.splunk.com/app/340/
12) sudo snort -A console -i eth0 -c snort.conf -l /var/log/snor
13) provide various types of nmap scans, and check Snort rules. And add Snort logs to Splunk.

Write a report with all of the steps and defend your assignment