Objective: Create a full Wazuh instance, integrated with SOAR by Shuffle along with a fully functional case management system through The Hive.

1. Create a full colored flow chart detailing all components and connections of system.
2. Create virtual machines and servers, and install necessary applications

* 1 Windows 10 Vm, on VmWare and 1 Ubuntu 22.04 VM.
* 1 cloud instance of an Ubuntu 22.04 server with Wazuh.
* 1 cloud instance of Ubuntu 22.04 server with The Hive.

3.Configure the Hive server, Wazuh server and Wazuh Agent On Windows 10 and Ubuntu 22.04.

* To configure the Hive we need to download its components and subsequently their components.Namely, ElasticSearch and Cassandra. Cassandra needs Java so we had to install that as well.
* Next we edit the configuration files for Cassandra, Elastic Search and the Hive.
* On our Hive server we will start all the services, on our Wazuh server we do the same.
* Login into both dashboards to confirm they are working
* We add our Windows 10 and Ubuntu 22.04 agents to our Wazuh dashboard through use of the dashboard prompts for adding an Agent and respective CLI’s

4. Configure Wazuh Dashboard for alerts, send telemetry to Wazuh from our agents and receive custom Mimikatz Alert from Windows and SSH auth failure from Ubuntu.

* We modify the ossec.conf files on our Windows 10 system to ingest Sysmon logs into our Wazuh dashboard. This is done by adding a tag with the location of the Sysmon program. Don’t forget to restart your service.
* We also need to modify the ossec.conf on our Wazuh server to ingest everything coming to it from our virtual machines. This is done by changing the parameters for logall to yes. The filebeat configuration file will need modification as well., enabling archives in filebeat.yml file. Don’t forget to restart your services
* In Wazuh we need to create an index pattern for archives so we can search our archives for all of the events that have occurred, regardless if Wazuh triggers an alert.
* We have found mimikatz events in our Wazuh dashboard, time to craft a custom alert for mimikatz event. To do this we need to modify our rules, which can be done from the dashboard or CLI. A rule must be added, to give alerts for mimikatz usage.
* Upon Running Mimikatz on our Windows 10 device, we get, as expected, an alert on our Wazuh Dashboard with the custom message “mimikatz Usage Detected”.
* With a public facing ip for Ubuntu machine it is constantly getting hit with ssh authentications. This is automatically detected by Wazuh, no special event confgiuration necessary

5. Connect our Shuffle(SOAR) platform to our lab, sending notifications to and creating cases

with the Hive. It will also send a response to our SOC Analyst(us) for responsive action.

* Begin by adding integration tags in the ossec.conf file. This can be found on the Wazuh website and we can integrate with webhook on Shuffle by using the webhook uri provided.
* For windows, using Shuffle we will extract the SHA256 hash from the file and check it’s reputation score with VirusTotal utilizing a few automations.
* Then it will be sent to The Hive for an alert.
* For Ubuntu we will follow a similar procedure. The ssh auth failure will be sent to Virus Total to check it’s source IP. From there it will be sent to the Hive for a case AND an email will be sent to the SOC analyst, requesting the responmsive action of blocking the source IP.