Part A: Practical Assignment (Homework)

Please select 1 of the three questions to do a practical assignment for and submit your code or written answers (pseudo-code as PDF) in a password-protected zip or share a GitHub link. Have a general read of at least one more question of the other questions to understand/discuss their position (the reading does not require any submission).

NOTE: The assessment is not going to be based on a working system but is intended to identify the framing of a solution and familiarity with Security Information and Event Management concepts.

These are the types of problems that one will be working with. Experience with the problems is not mandatory but the ability to work and interest to explore the space will be much preferred. Opportunities to learn will be provisioned as part of the role.

1. **Deploy at least 2 out of 4 of these projects**

Write scripts to configure and deploy local virtual machines (for virtual machines use either of these options Docker, Virtual Box, VMWare, AWS EC2, Azure, GCP e.t.c) with 2 of the 4 systems integrated

- TheHive
- Cortex
- Shuffle
- MISP

As an output, a scenario evidencing that the systems are working together should be provided e.g. running analysers for a malware hash (Hive + Cortex + MISP) or capturing observable from an API call (Shuffle + Hive + Cortex)

2. **Deploy Log Management with Wazuh to monitor system**

Write a script to configure and deploy Wazuh Server to a local virtual machine (for virtual machines use either of these options Docker, Virtual Box, VMWare, AWS EC2, Azure, GCP e.t.c). Also, deploy the Wazuh agent on another virtual machine and script out configurations to allow the agent to send logs to the server:

- Wazuh
- ElasticSearch
- Kibana

3. **Deploy Intrusion Alerting via Logs (ElasticSearch, ElastAlert and Slack)**

Write scripts to configure and deploy (for virtual machines use either of these options use options Docker, VirtualBox, VMWare, AWS EC2, Azure, GCP e.t.c) an alerting mechanism from ElasticSearch that publishes an alert to Slack or an Email. As part of the test, you can try to deploy a small web application that is sending weblogs to ElasticSearch. Create an ElastAlert Trigger that notifies the occurrence of 10 response code 4XX in a 1-minute window from a single IP address

- ElastAlert
- ElasticSearch