



AntWak Bootcamp

Incident Response Project

Project

1. Register on [Let's Defend](#), create a free account using email address registered with Antwak
2. Complete analysis of 5 free alerts & prepare 1 page report
3. Report must contain : Screenshot of dashboard, one para each for all alerts highlighting the summary of investigation and potential recommendation to avoid such incident
4. Analysis Steps:
 - Step 1 - Select an alert from Monitoring page
 - Step 2 - Create a case for investigation
 - Step 3 - Follow instructions on playbook
 - Step 4 - Turning off the alert at monitoring page

SOP's for the project



5. Following instructions are to be followed while doing the incident management project:-

- Screenshot of closed alerts should be provided
- Screenshot of the **dashboard with scores** should be provided. (<https://app.letsdefend.io/dashboard/>)
- Step by step process of a high severity level alert with screenshots should be displayed in the report.

6. Evaluation will done basis

- Total score received
- Average alert closure time
- Quality of the report submitted

Thank you