🛡️ **SECURITY ALERT MONITORING & INCIDENT RESPONSE**

**Submitted By:**

**Sushant Sudhakar Biranje**

**Role: Cyber Security Internship**

**Organization: Future Inters**

* **OBJECTIVE :**

To monitor simulated security alerts using Elastic Stack, identify suspicious activities in log data, classify incidents, and draft a structured incident response report.

🛠️ **USED TOOL’S :**

* OWSAP ZAP
* BURP SUITE
* SQL MAP

* **Perform Attack With Solution:**
* **Brute-force Login Attack**
* Repeated failed login attempt (401 status codes).
* **Solution:** implementcaptcha, account lockout, IP blocking.
* **SQL Injection**
* Presence of ‘1’=1
* **Solution:** Type validate input
* **Gained Skill**
* Applied structured KQL filters to isolate high-risk access patterns.
* Used Kibana Lens to visualize IP-based attack frequency.
* Conducted response payload analysis to detect fingerprinting risks.
* Documented findings in a professional report format with evidence-backed screenshots.