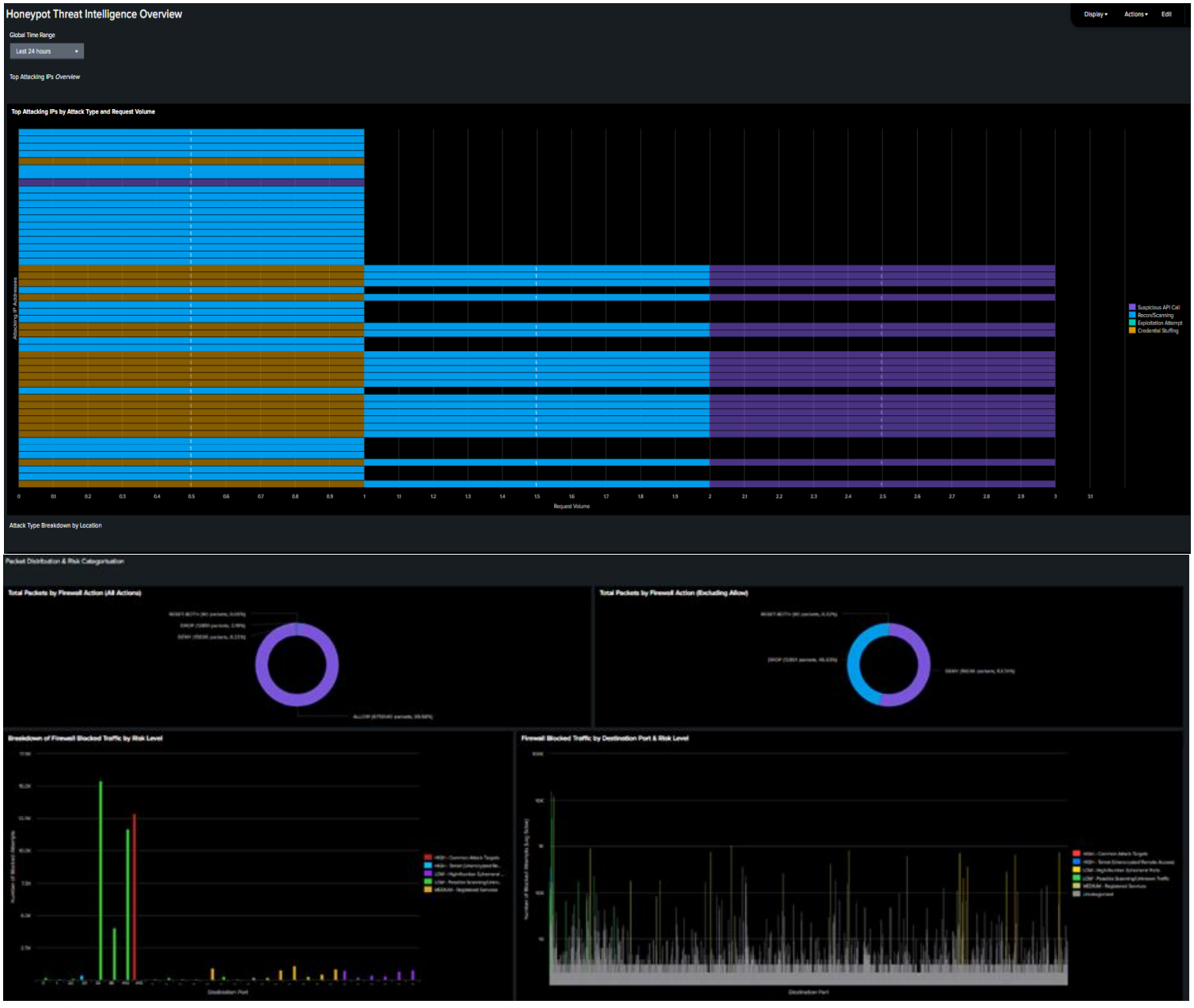
Joe Coffee – SOC Dashboard Portfolio

This portfolio highlights selected Splunk dashboards developed as part of a university-level SOC case study. Each visualisation was created using custom SPL queries to detect threats, track anomalies, and present data to support incident response and analysis.

Honeypot Logs (London & Singapore)

Mapped botnet-style and reconnaissance attacks by IP and region using Splunk 'geostats'. Panels showed threat type distribution and severity-based classification.

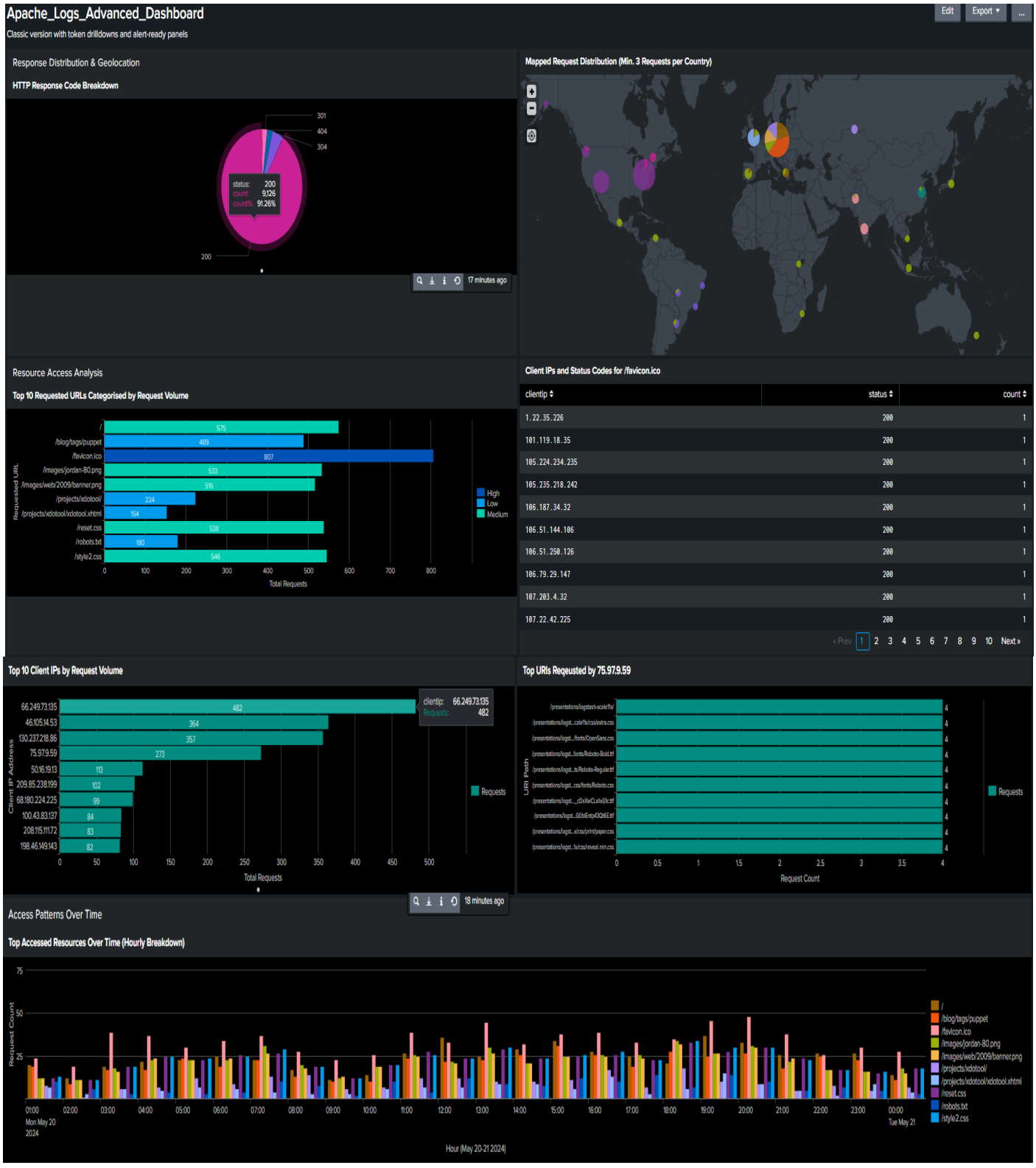


Linux Authentication Logs

Analysed failed vs successful logins, flagged top users and IPs, and used timecharts to reveal brute-force patterns.

Apache Web Server Logs

Tracked access to resources, 4xx error spikes, and mapped request origin globally. Revealed suspicious scan activity and URI anomalies.



Firewall Logs

Classified allowed/denied traffic, analysed port targeting (e.g. 23, 445), and calculated total data volumes. Helped expose scanning vs exfiltration attempts.

IDS Threat Monitoring - TII-SSRC-23 Dataset

Flagged most frequent attack subtypes, applied spike detection using 'streamstats', and forecasted malicious traffic with 'predict'. Sparkline trends tracked evolving threats.

Contact: josephcoffeecyber@gmail.com

LinkedIn: linkedin.com/in/joe-coffee1993