STORMBIRD

DETECTION

1 INTERROGATION

The system starts by gathering data from the user's request, examining various parameters to understand the context. It ensures that any suspicious or unexpected activity is flagged for further analysis.

2 REQUEST

The request is sent from the user to Stormbird for further detection, initiating the process of analyzing incoming traffic.

3 DDOS DETECTION

The system identifies patterns that match known DDoS attack strategies, such as high traffic volume or malicious traffic sources. Early detection minimizes the impact by activating preventative measures.

4 BOT DETECTION

The system analyzes behavior to distinguish human from automated traffic using advanced behavioral analysis and machine learning. Bots are detected through irregular patterns like repetitive actions or non-human response times.

5 RISK SCORE

A risk score is assigned based on the data collected and analyzed, indicating the likelihood of malicious intent. This score helps prioritize responses and determine the appropriate level of intervention.