■■ RDP Brute Force Detection – Executive Summary

Remote Desktop Protocol (RDP) brute-force attacks remain one of the most common entry points for ransomware and unauthorized access. This project analyzed honeypot logs to detect, visualize, and document brute-force activity targeting RDP services.

Key Findings:
- Continuous brute-force attempts were observed globally, primarily targeting the *Administrator* account.
- Attacks originated mainly from high-risk regions, including China and Russia.
- Geo-mapping provided visibility into attacker origins and patterns.

Detection Methods:
- Threshold-based detection of repeated failed login attempts.
- Geo-based detection of suspicious or high-risk countries.
- Identification of "impossible travel" (same account from different countries within 1 hour).

Lessons Learned:
- Even simple honeypots generate valuable intelligence for SOC monitoring.
- Normalizing logs into a data model enables portable SIEM use cases.
- Visualization improves situational awareness for both analysts and managers.

Next Steps:
- Expand detections to Windows Event Logs for deeper authentication detail.
- Map detections to MITRE ATT&CK; techniques (e.g., T1110 – Brute Force).
- Develop portable Sigma rules for SIEM-agnostic detection sharing.