Client: INFINA Finance
Report Type: Entity Behaviour Anomaly
Date: 2025-12-30
Threats:
- Unauthorized configuration changes detected on Fortigate firewall devices.
- Suspicious outbound connections to known malicious IP addresses.
- Privileged user activity outside business hours.
Vulnerabilities:
- Lack of MFA on firewall admin accounts.
- Inadequate monitoring of configuration changes.
- Weak alerting on abnormal user behavior.
Security Incidents:
- Multiple failed login attempts followed by successful admin access.
- Firewall policies modified to allow external access.
Recommendations:
- Enable MFA for all privileged accounts.
- Implement real-time configuration change monitoring.
- Review and restrict firewall rules immediately.