Notable Incident - 2

Title	Ransomware
Finding/Observation	• A ransomware attack occurred via a compromised VPN account, where the threat actor exploited a privileged binding account to escalate access. Systems, including hypervisors, servers, and endpoints, were impacted. The attacker disabled security monitoring, performed lateral movement, and encrypted critical files on the network storage and systems. While unauthorized data access was confirmed on several servers, the possibility of data exfiltration could not be ruled out due to limited network telemetry and the premature formatting of systems to facilitate recovery.
Risk Identified	• Significant operational disruption to trading activities and potential leakage of sensitive data. The incident highlights vulnerabilities in privilege management and a lack of forensic preservation protocols, which hinders the ability to definitively ascertain the extent of the data breach.
Possible Mitigation & Recommendation	• Affected systems were isolated to contain the threat, and critical servers were restored from backups to maintain business continuity. • Implement Multi-Factor Authentication (MFA) for all remote access and restrict privileges for service accounts. Establish a formal evidence preservation policy and enhance log retention. Finally, align the cybersecurity framework with regulatory resilience standards.