# *Notable Incident - 1*

| Title | Ransomware |
|---|---|
| **Finding/Observation** | • A regulated entity recently suffered a ransomware attack that encrypted servers and endpoints, disrupting business operations. A ransom note was discovered. Notably, certain core business systems remained unaffected because they were not integrated with the on-premises Active Directory, which effectively prevented the threat actor from moving laterally into those environments. |
| **Risk Identified** | • The incident caused significant operational downtime and posed a high risk of sensitive data exfiltration and the compromise of privileged domain administrator credentials. |
| **Possible Mitigation & Recommendation** | • The entity isolated infected systems, blocked malicious IPs and ransomware hashes, and reset all domain administrator passwords. Critical servers were restored from backups after thorough scanning for infection. Additionally, a new isolated network environment was established with an advanced EDR solution deployed for enhanced threat detection.<br>• The entity should implement broader network segmentation and a "Zero Trust" architecture, leveraging the isolation model that protected its core systems. Continuous threat intelligence monitoring is advised, alongside a comprehensive vulnerability audit to ensure full alignment with regulatory cybersecurity and resilience frameworks. |