CapStorm

CASE STUDY

ENTERPRISE SALESFORCE SECURITY BREACH DETECTION

GOVERN

PROBLEM

Security teams at this multinational manufacturer wanted an anomaly detection solution that automatically alerts abnormal Salesforce activity of a potential security breach. Specifically, analyzing Salesforce login history and event log files over a period of time across 5 Salesforce production organizations. Native Salesforce functionality had key limiters; fixed retention period for login history and recurring query timeouts when attempting to search log history.

SOLUTION

CapStorm's Salesforce data extract functionality replicated login history and event logs to the organization's relational database. The incremental nature of the solution meant data volumes, regardless of volume sizes, and frequent deltas could be stored locally. Data retention periods were set to meet security standards for each object, and CapStorms' View solution was leveraged to create a single point of query across all Salesforce orgs. This enabled automated cross-org analysis both in real-time and longitudinally to identify trends over long periods of time.

OUTCOME

Automated threat detection protects the business against both internal and external risks, including rogue employee or ransomware attempts. Analysis of login history trends over time also gives the business insight into user CRM utilization for individual users and user roles, making it simple to identify any groups that may need additional Salesforce training.

Multi-National Manufacturing Organization with 5+ Salesforce Production Orgs

CapStorm serves the Salesforce community with expert solutions for managing high-value, mission-critical data. Our customers gain autonomous use and control of data throughout their Salesforce environments, empowering enterprise value and confidence by managing data throughout its lifecycle.