LogSentinel

LogSentinel helps a large bank provide digital evidence

Business challenge

The Chief Information Security Officer of a large bank needs to be able to use logs as digital evidence in court cases regarding fraud.

Audit logs make sure that internal privileged actors cannot commit fraud without being detected. However, if logs themselves are unprotected, they can be deleted or modified by the privileged actor. Without additional protection, they may not have sufficient legal strength.

Solution

LogSentinel SIEM is integrated with the core banking system to provide immutability of the audit log.

The secure electronic timestamping used, combined with other cryptographic methods, turns the audit logs collected into **legally sound digital evidence**.

Key **Benefits**

01

EVIDENCE

The cryptographically protected and eIDAS-compliant audit log is a strong digital evidence

02

DETERRENCE

The inability of privileged users to cover their tracks serves as a deterrence for performing fraud

03

DETECTION

The rule-based and machine-learning anomaly detection is used to alert the infosec team on unusual patterns

About LogSentinel

LogSentinel is an innovative company that takes compliance and information security to the next level with cutting edge technologies

Audit trail

Store and analyze every business-relevant event

Integrity protection

Immutable, secure and provable to 3rd parties

Anomaly detection

Detect fraudulent and other anomalous behavior by people and systems

Full visibility

Gain full visibility over your IT stack, including legacy systems

LogSentinel