Elastic Stack

Wazuh integration with Elastic Stack comes with out-of-the-box dashboards for PCI DSS compliance and CIS benchmarking. You can do forensic and historical analysis of your alerts and store your data for years using a reliable and scalable platform. Optionally, this can even include your archived events rather than only your alert events.

The following requirements can be met with a combination of Wazuh + Elastic Stack:

10.5: Secure audit trails so they cannot be altered.
10.6.1: Review the following at least daily: All security events, Logs of all critical system components, etc.
10.7: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.