Functional requirements

The following requirements should be fulfilled:

- Fully featured logmanagement-system
  - receive logs in ANY logformat
  - Converting ogformats to support SIEM requirements
  - filtering unwanted logs
  - Protecting pipelines from overflooding
- Should fully integrate with Qradar and other SIEMs
- The following functionality should be available
  - buffering (in case of congestion/network outage/component failures)
  - filtering (should be possible anywhere in the pipeline)
  - logs should be searchable in a database-like datalake
  - logs should be stored to cold storage
  - encryption of data in transit AND data at rest should be supported
  - high availability, system should be able to fully recover from any type of intermittent failure
  - Redundancy: components should be replacable without service-degradation.
  - Solution should be platform-independent (OS/Hardware agnostic)
  - Components must be supported on latest OS/patchlsevels.
  - Components should be in active development/support.
  - platform should support log-transformation to meet Qradar log-standards
  - Each part of the data-pipeline should be auditable/monitorable.
  - Multi tenancy
  - Proven technology

Revision #4
Created 2026-02-02 11:05:34 UTC by Admin
Updated 2026-02-02 11:48:03 UTC by Admin