

Abstract

TGDetect 3.0 contains the following

Note: You can upgrade from any previous release of TGDetect.

Enhancements

- MSGQMON logic to reduce CPU Usage
- Real-time events in CEF and LEEF are formatted incorrectly.
- History Log (QHST) and Message Queue monitor every severity conversion in *SYSLOG format is incorrect.
- Option not available to start batch SIEM from current timestamp.

Bug Fixes

- Real-time events Forwarded SIEM is missing Job User and Job Name.