

ABSTRACT

LOG ANALYSIS SYSTEM

A log analysis system includes a first processor unit, a second processor unit, a third processor unit, and a fourth processor unit. The first processor unit normalizes the detection log acquired by an acquirer, allocating the detection log into predefined monitoring target units, and outputs the monitoring target units. The second processor unit appends common information based on a predefined rule to each of the monitoring target units of the detection log output from the first processor unit, arranges the monitoring target units into information granularities based on the content of the detection log and common information, and outputs the monitoring target units as analysis unit information. The third processor unit gathers the analysis unit information output from the second processor unit and setting detection target event candidates based on a predefined rule, determines whether or not the detection target event candidates are detection target processes having the specific quality based on a predefined rule, and outputs the detection target event candidates and the determination results. The fourth processor unit outputs the detection target event candidates and the determination results output from the third unit in a predefined output format.

FIG. 1