

ABSTRACT

Method and a server for determining a response to cyberthreats are provided. The method comprises: training a neural network to identify false-positive alert messages by: generating a cyberthreat database, the generating including acquiring, from a plurality of cyber-intelligence sources, data associated with a plurality of cyberthreats; acquiring a plurality of training alert messages generated by information security systems, using internal alert data and host data associated with a given training alert message to query the cyberthreat database to identify enrichment data associated with the given training alert message; generating a respective vector for the given training alert message using: (i) the internal alert data; (ii) the host data; (iii) the enrichment data of the given training alert message; and (iv) a respective label thereof; and feeding the respective vector to the neural network to train the neural network to determine whether a given in-use alert message is false-positive.

Fig. 1A