ABSTRACT

The computer network is the media information that is evolving so rapidly, almost all communication activity using computer networks as a medium transformation information. But there are things that must be considered in the use of computer networks, namely the large number of current data that is coming out in, malicious traffic is an abnormal incident on network traffic that may harm your computer. To find out the condition of normal and abnormal tissue is needed for monitoring surveillance systems, process, and control. To resolve the issue at the end of this Project was undertaken monitoring system by using the maltrail application that makes use of publicly available list that contains the path of dangerous or suspicious in General, along with the trace static reports are collected from AV and special user-defined list, the trail can be anything from domain name, URL or IP address. Maltrail ter-application integration with a variety of tools, namely sensors, servers, and clients. The sensor is a component for monitoring traffic to Find "trail " that have been signaled in a blacklist, and the server will store all events (i.e. log entries) in the period (24 h) which will be transferred to the client in CSV form. Then the client in the form of a web browser as a web interface for monitoring via the web that displays data in the form of presentations such as threats, incidence, source, and by accessing the http://127.0.0.1:8338.

Keywords: network, malicious traffic, system monitoring, maltrail, sensor, a server, a client.