Wireless Intrusion Detection Solution

Wireless Sensor Constantly scan each Wireless LAN radio channel and screen all the radio packets in the air. These packets will then be forwards to the NMS for analysis. The Wireless Sensor detects unauthorized access or other interference into the network.

WNCS-233 NMS Network Management Software manages the Wireless Sensor of the wireless intrusion system. The SNMP Read function allow the software to read the status and configuration status of each equipment, such as network traffic, number of wireless association, and other useful information. By monitoring the activities picked-up by the Wireless Sensor, it is able to determine if there is wireless intrusion.

WNCS-233 NMS is also able to manage and perform firmware upgrade of all Wireless Sensor remotely.

WNCS-SIEM Analyser Security Incident Event Management is a web-based, real-time event log, syslog management solution that collects security events, activities logs and alerts generated by the network, hardware and applications. It conducts a correlation analysis on these logs to determine if there is a security attack or intrusion. When a security event is detected, SIEM will trigger a security alert.

WNCS-SIEM Analyser helps organizations to collect, analyse, correlate, report, archive, and search logs without any hassle. It offers a centralized repository to collect and archive the machine generated logs, enabling network administrators to quickly troubleshoot and identify the root cause of IT problems, and audit trail on security events for cyber forensic purposes.

Typical Wireless Intrusion Detection Network Diagram