3.2 Network Monitoring

SNMP Manager + SNMP Agent + MIB = Monitoring

SIEM	Security Information and Event Management together
SEM	Security Event Management
SIM	Security Information Management
Unencrypted SNMP	V1, V2 and V2c
Encrypted SNMP	V3
SNMPv1, v2c	Community String
SNMP v2	No community string
Syslog	Performance monitor in MacOS and Linux, 514
CARP	Cache Array Routing Protocol for proxy servers to change information
SIEM	SEM+SIM
Traffic Analyzer	To analyze log files of webserver
Syslog 0	Emergency code 0
Syslog 1	Immediate action is required message
Syslog 2	Critical condition
Syslog 3	Error condition
Syslog 4	Warning message
Syslog 6	Informational message
Malformed/Unreadable/Discards	Packets which are not accepted by the interface monitor
Data Aggregation	Process of gathering information from multiple logs
Correlation	Process of linking logged events with

	common attributes
Retention	Long term storage of data
OID(Object Identifiers)	The numbers given to the logs in MIB
Ad Hoc Discovery	One-time scan of a range of IP addresses to determine if they are in use