Table 1: Ranking of top 20 entries according to the number of citations in Google Scholar

Reference	Title
[?]	Alert correlation in a cooperative intrusion detection framework
[?]	Constructing attack scenarios through correlation of intrusion alerts
[?]	Comprehensive approach to intrusion detection alert correlation
[?]	Clustering intrusion detection alarms to support root cause analysis
[?]	STATL: An attack language for state-based intrusion detection
[?]	Managing Alerts in a Multi-Intrusion Detection Environmen
[?]	Techniques and tools for analyzing intrusion alerts
[?]	Fusing a heterogeneous alert stream into scenarios
[?]	Mining intrusion detection alarms for actionable knowledge
[?]	Modeling multistep cyber attacks for scenario recognition
[?]	Statistical causality analysis of infosec alert data
[?]	Correlation of intrusion symptoms: an application of chronicles
[?]	Mining alarm clusters to improve alarm handling efficiency
[?]	Analyzing intensive intrusion alerts via correlation
[?]	Learning attack strategies from intrusion alerts
[?]	Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts
[?]	Attack Plan Recognition and Prediction Using Causal Networks
[?]	Building Attack Scenarios through Integration of Complementary Alert Correlation Method
[?]	Plan recognition in intrusion detection systems
[?]	Correlating intrusion events and building attack scenarios through attack graph distances