CDAC Project Literature Review

S.no	Title	Year	Techniques Used	Results	Limitations
1.	A New Alert Correlation Algorithm Based on Attack Graph	2021	Attack Graph (AG), Alert Correlation, Aggregation, Floyd-Warshall Algorithm	The proposed AG-based correlation algorithm identified multiple attack scenarios, reducing the number of false-positive alerts by 67.86%. It successfully filtered suspicious alert sets.	The approach may produce false positives in certain cases, especially if alerts are categorized differently. Parameter tuning for aggregation threshold affects detection accuracy.
2.	A survey on artificial intelligence techniques for security event correlation	2022	AI-based techniques (Rule-based, Semantic models, Graphical models, Machine Learning, Hybrid models)	Provided systematization of AI-based security event correlation models; highlighted the development prospects of hybrid models and discussed challenges in the field	The survey emphasized the challenges of defining the logic in multi-step attacks and handling large amounts of heterogeneous data, highlighting future areas for improvement.
3.	Graph-based Event Correlation for Network Security Defense	2019	Graph Theory, Graph Databases, Network Intrusion Detection System (NIDS), Network Security Monitoring (NSM), Event Correlation	The study demonstrated an architecture for collecting and transforming security events from multiple sources (NIDS, NSM, telemetry) into a graph database.	The research was conducted in a limited simulation environment, restricting the evaluation of the model's efficacy on larger enterprise networks. The study also involved a narrow range of attack scenarios, limiting the diversity of the attack surface.
4.	Intrusion Detection with Data Correlation Relation Graph	2008	CRG Construction Algorithm , CRG for Neptune (Synflood) Attack	The proposed approach uses Correlation Relation Graphs (CRG) for detecting attacks like Synflood. The method achieved high detection rates with Synflood attacks, with results showing 95.5% detection and a low false alarm rate of 0.38%.	The approach is primarily misuse-based, meaning it relies on known attack patterns and may not detect novel attacks. Furthermore, the CRGs with fewer nodes tend to generate more false alarms due to weaker correlation links.
5.	Evaluating LLM Agents for Event Forecasting	2024	Large Language Models (LLMs), MIRAI Benchmark,	Results showed a decline in prediction accuracy with increased temporal	Limited number of LLM models were tested, basic API functions, and cost

			GDELT1 Event Database, API Tool Integration, Temporal Forecasting	distance, especially beyond 30 days.	constraints led to high variance in experimental results.
6.	Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing	2019	Graph-Based Analysis, Bayesian Networks, Markov Models (HMM, MDP, POMDP), Cost Optimization, Uncertainty Analysis	The paper surveys various methods for analyzing attack graphs, emphasizing data and knowledge processing aspects. It reviews different approaches to constructing and analyzing attack graphs, which model potential security threats and vulnerabilities in systems.	Bayesian and Markov models require extensive data and are complex, especially with approximation algorithms. Graph-based methods, while simpler and more scalable, may not handle uncertainties and correlations as effectively.