



Graph Analytics and Network Analysis

Course: Link Analysis, Community Detection and Graph Databases



Graph Analytics and Network Analysis Course: Link Analysis, Community Detection and Graph Databases

Introduction:

Graph analytics and network analysis with link analysis, community detection and graph databases is a 5-day course for investigation, intelligence, financial crime and data science staff, ending with a Network Investigation and Analytics Plan for a case organisation. Connected risks such as collusive supplier clusters, mule account chains and single points of failure in supply tiers stay hidden when records are analysed one row at a time. Nominees already query data in SQL or Python; the course runs as hands-on labs on a property graph database and network analysis libraries. CoreConcept Training Center delivers this graph analytics course.

Course Objectives:

- Frame investigative and operational questions as graph problems and prepare edge lists, adjacency data and bipartite networks
- Design a labelled property graph schema, load records and write Cypher queries that traverse multi-hop relationships
- Rank key actors with degree, betweenness, closeness, eigenvector and PageRank centrality and explain what each score shows
- Detect communities and rings with Louvain, Leiden, label propagation and connected components, and trace paths and flows between entities
- Apply link prediction and node embeddings to add graph features to classification models and diagnose supernode and sampling distortions
- Produce a Network Investigation and Analytics Plan setting data sources, graph schema, algorithms and review steps for a case organisation

Target Audience:

- Investigation and intelligence staff responsible for tracing links between persons, accounts and companies
 - Financial crime analysis staff responsible for reviewing transaction networks and suspicious activity referrals
 - Data science staff responsible for building features and models from relationship data
 - Supply chain and procurement analysis staff responsible for mapping supplier tiers and dependencies
 - People analytics staff responsible for studying collaboration and communication patterns across units
-

Course Outline:

Day 1: Network Thinking, Graph Structures and Investigative Questions

- Nodes, Edges, Directed and Weighted Graph Structures Explained
- Adjacency Matrix and Edge List Data Preparation
- Bipartite Networks Linking People, Accounts and Addresses
- Degree Distribution, Density and Clustering Coefficient Reading
- Investigative Question Framing for Connected Data Problems

Day 2: Property Graph Modelling and Cypher Query Labs

- Labelled Property Graph Schema for Transactions and Parties
- Cypher MATCH Patterns for Multi-Hop Relationship Traversal
- Bulk Import of CSV Records Into a Graph Database
- Entity Resolution Rules Merging Duplicate Persons and Companies
- ISO GQL Standard and openCypher Query Portability

Day 3: Centrality, Community Detection and Path Analysis

- Degree, Betweenness and Closeness Centrality for Key Player Ranking
- PageRank and Eigenvector Centrality for Influence Scoring
- Louvain Modularity and Leiden Refinement for Community Detection
- Label Propagation and Connected Components for Ring Discovery
- Shortest Path and Weighted Flow Tracing Between Suspect Entities

Day 4: Graph Machine Learning, Link Prediction and Analytical Pitfalls

- Link Prediction Using Common Neighbours and Adamic-Adar Scores
- Node2Vec Node Embeddings as Features for Classification Models
- Graph Neural Network Concepts for Node and Edge Labelling
- Supernodes, Sampling Bias and Resolution Limit Troubleshooting
- Network Visualisation Layouts and Evidence-Grade Link Charts

Day 5: Lab Build of the Network Investigation and Analytics Plan

- Fraud Ring Lab Detecting Shared Devices and Collusive Accounts
 - Money Laundering Network Lab Tracing Layering Chains and Mule Hubs
 - Supply Network Lab Locating Single-Point Supplier Dependencies
 - Organisational Network Lab Mapping Collaboration Bottlenecks and Brokers
 - Network Investigation and Analytics Plan Completion and Peer Review
-

Skills You Will Gain:

- Graph Data Modelling
- Cypher Query Writing
- Centrality Analysis
- Community Detection
- Path and Flow Tracing
- Link Prediction
- Graph Feature Engineering
- Link Chart Presentation

Why Attend This Course:

- Deliver a Network Investigation and Analytics Plan for a case organisation to the head of investigations, the analytics lead or the risk committee
- Decide which centrality, community or path algorithm answers a given investigative question and how to read its output
- Avoid missed collusion rings, misleading supernode results and link charts that fail to stand up in case review
- Coach analysts and investigators in Cypher patterns, algorithm choice and graph feature design using the lab queries

Conclusion:

Back at work, the participant hands the Network Investigation and Analytics Plan to the head of investigations, the analytics lead or the risk committee, who use it to approve a graph pilot, the data sources to link first and the algorithms to run on priority cases. Investigation teams can reuse the Cypher patterns and link chart conventions on live referrals. After the first cycle of cases, the unit should review how many detected communities were confirmed, how many leads came from path or link prediction results and whether the graph schema needs new entity or relationship types.

Frequently Asked Questions FAQ:

What should participants know before a graph analytics and network analysis course?

Participants should be comfortable querying data in SQL or a scripting language such as Python and reading basic statistics. No prior graph database experience is needed. An anonymised list of entities and relationships from their own work makes the labs and the plan more relevant.

How does graph analytics and network analysis differ from a knowledge graph course or a fraud detection management course?

This course analyses network structure with centrality, community and path algorithms. Knowledge graph courses build semantic schemas and ontologies for data integration, while fraud detection management courses set detection programmes, thresholds and alert workflow; both treat network algorithms only briefly.

Why does community detection matter in graph analytics and network analysis?

Community detection groups entities that interact more with each other than with the rest of the network. In investigations it exposes rings of accounts, suppliers or persons acting together, which single-record rules miss, and gives investigators a cluster to review rather than isolated alerts.

What do participants take back from the graph analytics and network analysis course?

Participants take back a Network Investigation and Analytics Plan for a case organisation, with a graph schema, data source list, algorithm choices for each question, review steps for results, and lab Cypher queries and link chart conventions to reuse with their own teams.
