Security Risk & Data Analytics in Due Diligence

1. Introduction to Security Risk in Due Diligence

• Defining security risk vs. IT risk
• The role of due diligence in risk management
• Differences between compliance checks and security-driven checks

2. Security Risk Identification in Human & Organizational Contexts

• Identifying insider threats (employees, contractors, vendors)
• Organizational vulnerabilities (governance, culture, fraud exposure)
• Environmental and geopolitical factors affecting security

3. Background Checks as a Security Risk Tool

• Types of background checks: criminal, financial, employment, education
• Social media and online footprint analysis
• Reference checks and reputation analysis
• Red flags and escalation protocols

4. Enhanced Due Diligence (EDD)

• Standard due diligence vs. enhanced due diligence
• Beneficial ownership and corporate structure mapping
• Screening against sanctions, PEPs (Politically Exposed Persons), and watchlists
• Investigating shell companies, offshore holdings, and hidden affiliations

5. Threat Modeling for Human & Corporate Risks

• Applying threat modeling beyond IT (STRIDE/PASTA adaptation)
• Mapping threat actors: insiders, competitors, hostile states, organized crime
• Risk scenarios: fraud, data leakage, sabotage, reputation damage
• Attack surface analysis: HR processes, vendor ecosystems, partnerships

6. Investigative Tools & Techniques

• Open Source Intelligence (OSINT) in background checks
• Commercial databases and watchlist tools

• Financial forensics and document verification
• Red-teaming and simulated adversarial research

7. Data Analytics for Risk Detection *(New)*

• Leveraging big data for identifying hidden risk patterns
• Predictive analytics for fraud detection and insider threat identification
• Correlating cross-domain data (HR, finance, operations) to flag anomalies
• Role of AI/ML in proactive due diligence

8. Data-Driven Continuous Monitoring *(New)*

• Using real-time analytics to detect behavioral or transactional red flags
• Automating vendor and employee monitoring through dashboards
• Risk heatmaps and visualization for decision-makers
• Integrating analytics with enterprise security platforms

9. Legal & Ethical Considerations

• Data privacy laws (GDPR, CCPA, etc.)
• Limitations of background checks (consent, scope, bias)
• Balancing ethics with proactive risk management

10. Risk Scoring & Decision Frameworks

• Building a risk profile for individuals and organizations
• Using weighted scoring models (likelihood × impact)
• Integrating due diligence outcomes into corporate risk registers

11. Case Studies & Real-World Examples

• Background check failures leading to major breaches
• Vendor due diligence lapses and supply chain compromise
• Insider threat incidents uncovered through proactive checks

12. Best Practices & Continuous Monitoring

• Ongoing monitoring vs. one-time checks
• Integrating background checks into onboarding and vendor management
• Leveraging AI and automation in due diligence
• Establishing a feedback loop into enterprise security strategy