

B Interview Codes and Themes

Table 10 provides a summary of our codebook.

Table 10: Consolidated Summary of Themes and Codes

Theme	Codes
Attribution Methods	Low-Level Indicators, Ransomware Analysis Methods, High-Level Indicators are Generic, Tools, Detection Methods, Darknet Investigation, Modus Operandi supports Attribution, Ransomware Code Patterns, High-Level Indicators are Valuable, Attribution by Activity Clustering, Ransomware groups outing themselves with ransom notes, Root Cause Analysis, High-Level Indicators, Communication Channel Analysis, Infrastructure Analysis, Attacker Profiling, Open-Source Intelligence for Attribution, Different Forms of Attribution, Pyramid of Pain in Attribution, High-level indicators as a way to conceptualize behavior, Strengths of the Attribution Process, group-level attribution
Attribution Objectives	Stopping at Group-Level Attribution during Investigations, Benefits of Attribution
Challenges with Attribution	Challenges in Individual-Level Attribution, Legal Challenges in Attribution, Confidence Levels in Attribution, Added Value of Active Ransomware Attribution, Ransomware Rebranding, Improvement Points in Attribution, Performing Country-Level Attribution, Complexities due to Data Fragmentation, Complexity in Correlating Indicators, Lack of Attribution Data, Attribution Accuracy, Attribution requires diverse knowledge and sources of information, Reputational Repercussions of Misattribution, Organizations Publishing Inaccurate Attributions
Ethical and Legal Considerations	Legal Considerations, Political Repercussions of Attribution, Ethical Considerations
Knowledge Management and Collaboration	The Need for an Centralized Knowledge Management Platform, Essence of Collaboration, Improving using Information Sharing
Operational Constraints	Resource Constraints in investigations, Differences Law Enforcement and Industry
Sanction Compliance	Attribution for Sanction Checks, Consequences of Inaccurate Sanction Screening, Verification against Sanction Lists, Legal Ambiguities within Sanction Screening
Threat Actor Motives and Behaviors	State vs. Criminal Actors, Ransomware Actor Motives, False Flag Operations, Ransomware Observed Procedures, Ransomware-as-a-Service, Ransomware Group Brand and Reputation
Challenges with Indicators	Complexity in Correlating Indicators, Lack of Attribution Data, Attribution Accuracy
Threat Actor Typologies	Nation-State Actors, Cybercriminal Groups, Hacktivists