For a project focusing on cybersecurity threats on the Internet of Things (IoT) for vehicle automation, mixed data collection approaches can be considered, and a conclusive research design approach could be used as per the BRM (2019) research designs.

Literature Review: Conducting a thorough literature review would be essential to understand existing research, identify common cybersecurity threats, and explore mitigation strategies specific to IoT and vehicle automation.

Expert Interviews: Interviewing experts in cybersecurity, IoT, and automotive industries could provide valuable insights into emerging threats, current practices, and potential vulnerabilities in vehicle automation systems.

Case Studies: Analyzing real-world case studies of cybersecurity incidents in IoT-enabled vehicles can offer concrete examples of threats and their impact on vehicle automation systems.

Simulation and Experimentation: Utilizing simulation tools or building experimental setups to simulate IoT environments and vehicle automation systems can help in testing various attack scenarios and evaluating the effectiveness of security measures.

Data collection methods may include:

Document Analysis: Gathering data from technical reports, white papers, industry standards, and academic publications to understand the landscape of cybersecurity threats in IoT for vehicle automation.

Interviews and Surveys: Collecting qualitative data through interviews with experts and stakeholders, as well as conducting surveys to gather insights into perceptions, practices, and challenges related to IoT security in automotive systems.

Observations: Observing IoT-enabled vehicles in real-world settings or controlled environments to identify potential security vulnerabilities and observe user behaviors related to cybersecurity practices.

Simulation Data: Collecting data generated from simulations or experiments conducted to mimic IoT and vehicle automation scenarios, including data on attack vectors, system responses, and performance metrics.

Skills required for this project may include:

Understanding of Cybersecurity Concepts: Knowledge of cybersecurity principles, threats, and mitigation strategies, particularly in the context of IoT systems and automotive cybersecurity.

Research Skills: Ability to conduct comprehensive literature reviews, analyze technical documents, and synthesize information from various sources to inform research findings.

Data Collection and Analysis: Proficiency in qualitative research methods, such as conducting interviews, surveys, and observational studies, as well as analyzing qualitative data to extract meaningful insights.

Domain Expertise: Familiarity with IoT technologies, vehicle automation systems, and related standards and protocols to understand the intricacies of cybersecurity threats in this domain.

Communication Skills: Effective communication skills to convey research findings, engage with stakeholders, and disseminate knowledge to both technical and non-technical audiences.

By employing a combination of these methods and data collection approaches, along with developing the necessary skills, a comprehensive understanding of cybersecurity threats in IoT for vehicle automation can be achieved, contributing to the development of effective security solutions and practices in this critical domain.

Reference:

BRM (2018) Data Collection Methods. Available at: <https://research-methodology.net/research-methods/data-collection/> [Accessed 1 April 2024].