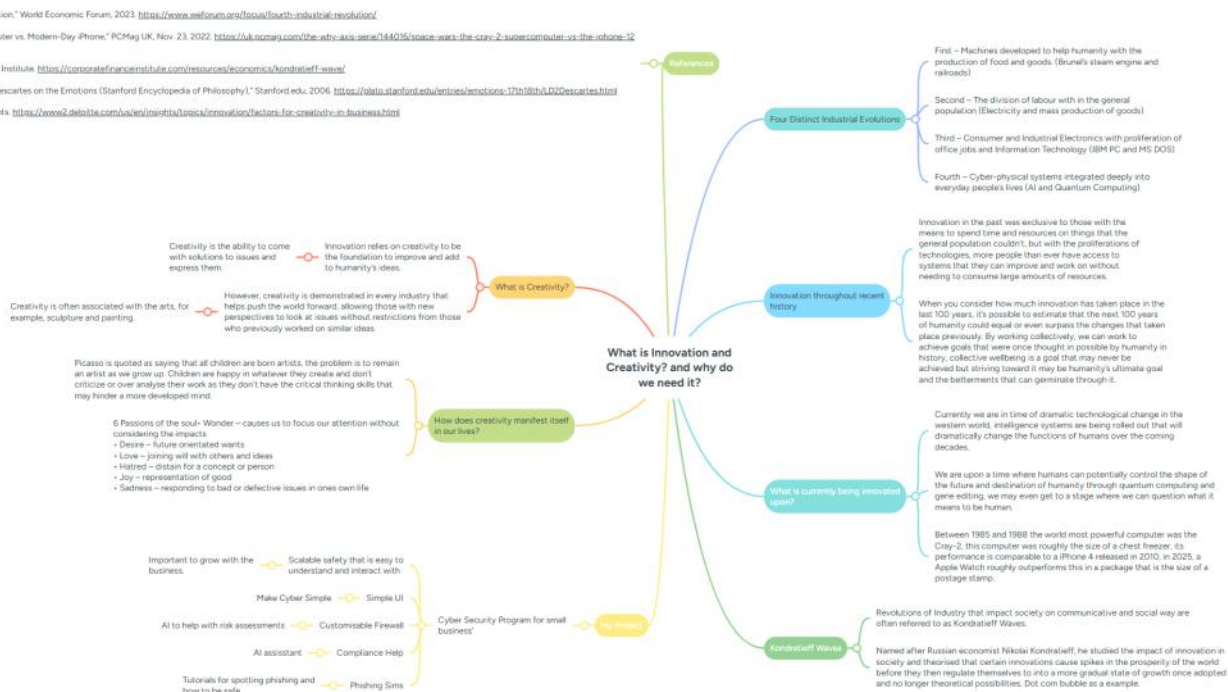


Task 1: Ideation & Mind Map

03 June 2025 14:15



<https://mm.tt/mmap/37330285547rozmljgw6m>
use this link to view mind map

References

- [1] World Economic Forum, "Fourth Industrial Revolution," World Economic Forum, 2023. <https://www.weforum.org/focus/fourth-industrial-revolution/>
- [2] C. Steele, "Space Wars: 80s CRAY-2 Supercomputer vs. Modern-Day iPhone," PCMag UK, Nov. 23, 2022. <https://uk.pcmag.com/the-why-why-series/144016/space-wars-the-cray-2-supercomputer-vs-the-iphone-12> (accessed Jun. 03, 2025).
- [3] CH Team, "Kondratieff Wave," Corporate Finance Institute. <https://corporatefinanceinstitute.com/resources/economics/kondratieff-wave/>
- [4] "17th and 18th Century Theories of Emotions > Descartes on the Emotions (Stanford Encyclopedia of Philosophy)," Stanford.edu, 2006. <https://plato.stanford.edu/entries/emotions-17th18th/1.02Descartes.html>
- [5] "Factors for creativity in business," Deloitte Insights. <https://www2.deloitte.com/us/en/insights/topics/innovation/factors-for-creativity-in-business.html>

Task 2: Aims and Objectives

03 June 2025 14:15

Aim

The aim of this project is to develop a scalable Cybersecurity solution for small to medium sized businesses that can not only protect these businesses but also work to educate and develop skills necessary to work within the cybersecurity industry and internally train users to work within the industry.[1]

Objectives

1. Design and Develop a Scalable SIEM Solution
 - Create a modular SIEM platform tailored to small and medium businesses, with features like automated log analytics, dynamic threat detection and automated alerts.
 - Ensure the solution is cost-effective, easy to deploy and scalable to different business sizes.
2. Implement Cybersecurity Education
 - Integrate a educational component into the SIEM platform, offering interactive tutorials, threat simulations and best practices for end-users.
 - Develop role-based training to improve internal cybersecurity awareness and capabilities.
3. Enhance Threat Detection and Response
 - Utilising machine learning (AI) and rule-based log analytics to identify attack types and threats (phishing, malware, insider threats).
 - Live feedback and remediation steps to users when threats are detected.
4. Workforce Development in Cybersecurity
 - Offer certifications in Cybersecurity or skill badges for users who complete advanced training modules.
 - Use educational institutions or industry bodies to make sure training aligns with recognised cybersecurity standards and qualifications. (CompTIA Security+, NIST).
5. Evaluate and Optimize the Solution
 - Conduct testing with 3-5 businesses to assess usability, effectiveness, and outcomes of education contained in the program.
 - Gather feedback from businesses to refine the SIEM's functionality and educational content before full-scale deployment in industries.

Research Philosophy Justification

A research philosophy is a fundamental set of beliefs that guides how you approach research for any project. It's the framework that shapes your entire how you discover and learn.[2]

The Three Main Research Philosophies:

1. **Positivism** (Objective/Scientific)

- Believes reality is fixed and measurable
- Using quantitative methods (surveys, experiments)
- Seeks universal laws and cause-effect relationships
- Example: Measuring exact improvement in threat detection rates

2. **Interpretivism** (Subjective/Contextual)

- Believes reality is socially constructed
- Uses qualitative methods (interviews, observations)
- Focuses on meanings and experiences
- Example: Understanding how small business owners perceive cyber threats

3. **Pragmatism** (Practical/Problem-Solving) [3]

- Focuses on "what works" rather than abstract principles
- Uses mixed methods (both quantitative and qualitative)
- Concerned with solving real-world problems
- Example: Creating a SIEM tool that actually helps small businesses, testing both its technical performance AND user experience

My project adopts a pragmatic research philosophy, making it ideally suited to the dual objectives of developing a technical SIEM solution while advancing cybersecurity education.

Pragmatism is oriented towards practical results, this is key to enabling a scalable solution by gaining understanding of how the project can solve the problems that it aims to solve through results on the fly. Flexible methodologies are key to getting a good result, analysing both quantifiable and qualitative data through detection rates and interviews and questionnaires.

Pragmatism also offers a focus on consequences that the other philosophies don't allow for, this is key when aiming for a security solution due to the consequences that can occur if the project was ineffective (loss of data and legal ramifications). Iterative development means that the project can be moulded to the users as the research is conducted, creating a built-in ability to scale to different businesses as per the aims and objectives of the project.

If this study were to use a positivist philosophy, it would have focused on controlled experiments and statistical generalisation, neglecting the contextual challenges faced by small businesses. Also, an interpretivist approach might have focused heavily on subjective user experiences at the expense of quantifiable security improvements. Pragmatism overcomes the issues with other philosophies, ensuring the research remains both in depth and relevant to its target audience.

Bibliography

[1]

O. Doody and M. Bailey, "Setting a research question, aim and objective," *Rcni.com*, 2016. <https://journals.rcni.com/nurse-researcher/setting-a-research-question-aim-and-objective-nr.23.4.19.s5>

[2]

I. Tshabangu, S. Ba, and S. M. Madondo, *Approaches and Processes of Social Science Research*. IGI Global, 2020.

[3]

M. Bacon, *Pragmatism: An introduction*. Cambridge: Polity Press, 2012.

Task 3: Strategies to Enhance Validity, Reliability, Generalisability, and Ethical Considerations

03 June 2025 14:15

To ensure the scalability of this study, different strategies will be used to address validity, reliability, generalisability, ethical considerations for the development and evaluation of both the SIEM solution and the cybersecurity focused educational aspect of my project.

Validity

Validity is the accuracy of findings from the research when compared to real-world results. Strategies to improve validity include;

Triangulation

Combining multiple data sources (log analytics, user feedback, assessments) to cross verify results [1]

When using multiple data sources/methods to confirm results, for example SIEM logs (quantitative) show a 40% decrease in phishing attacks, user interviews tell us that employees are better at understanding how to spot phishing emails and pre/post testing shows that a 35% increase in knowledge of phishing tactics. When all these results are compared we can find that when all three data points align in a positive manner we can conclude that the positive results are valid.

Member Testing

When researchers share their interpretations of interview data with the original participants, for example by sending a summary stating "Users found the SIEM dashboard confusing" back to the interviewees, then those participants confirm this interpretation by responding "Yes, the alerts were too technical," this verification process ensures the research's findings accurately reflect the participant's true experiences. By having subjects validate the findings, the credibility of our qualitative data is much better and reduces researcher bias, making the study's insights more trustworthy. [2]

Reliability

Reliability is the ability to ensure that the tests are consistent with the measurements of other relevant studies (ensuring that participants in the study are given consistent ways to measure their adherence to the information). Strategies to improve reliability include;

Standardised Measurements

When establishing consistent evaluation methods, like using identical SIEM detection rules across all test environments (applying the same threshold of 3 failed login attempts to trigger brute-force alerts) and administering structured questionnaires with fixed response scales (Rate alert clarity from 1-5), this standardisation minimizes measurement differences [3]. The uniformity ensures that when a observed 25% reduction in incident response time across businesses, we can attribute this improvement to actual system performance rather than inconsistent assessments.

Test/Retest

When applying the test-retest method, such as readministering the same 20 question cybersecurity quiz to staff after a 14-day interval and obtaining correlated scores

between initial and follow-up assessments, this stability confirms that our knowledge measurement tool captures enduring learning outcomes rather than temporary recall [4]. The strong correlation indicates employees retained core concepts like phishing identification techniques, making the conclusions dependable.

Generalisability

While small business all vary, the program design has to reflect this, this is known as generalisability. Strategies to improve generalisability include:

Diverse Sampling

The research would incorporate businesses from multiple sectors and varying scales - retail, healthcare, and professional services - to evaluate whether the cybersecurity solution shows consistent effectiveness across different operational environments. This cross-industry comparison would help determine if the tool's benefits extend beyond specific business needs.

Defined Boundaries (Methodological Framework)

Taking inspiration from [5] *Basics of Research Methodologies* recommendations, the research would explicitly limit participation to organizations meeting specific criteria: 5-50 employees, under £2M annual revenue, and no dedicated IT staff. These parameters would create clear guidelines for assessing the potential applicability of findings to similar small business contexts.

Bibliography

[1]

L. M. Given, *The Sage encyclopedia of qualitative research methods*. London: SAGE, 2008.

[2]

"RWJF - Qualitative Research Guidelines Project | Member checking | Member Checks," *Qualres.org*, 2019. <http://www.qualres.org/HomeMemb-3696.html>

[3]

A. J. Laver Fawcett, *Principles of assessment and outcome measurement for occupational therapists and physiotherapists theory, skills and application*. Chichester Wiley, 2007.

[4]

S. A. McIntire and L. A. Miller, *Foundations of psychological testing : a practical approach*. Thousand Oaks: Sage Publications, 2007.

[5]

A. Gopalakrishnan, *Basics of Research Methodologies*. RK Publication, 2025.