

Chapter 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

Based on the experimental results, several conclusions can be made:

1. Integrating maturity assessments into the DevSecOps process ensures that applications comply with necessary security standards, particularly those related to UU PDP, before deployment. This approach helps organizations more effectively mitigate potential data breaches and credential leaks along with rapid development application.
2. Regular security assessments—such as VAPT, SAST, and DAST—are critical to identifying vulnerabilities during development. Proactive monitoring adds an extra layer of defense once the application is live, detecting any new threats that may arise in real-world environments.
3. The specific strategy for implementing UU PDP in DevSecOps involves integrating security into the CI/CD pipeline and conducting maturity assessments to ensure the application has implemented the necessary security measures. This approach uses ISO 27001 as a benchmark, along with a risk-based framework to enhance compliance and security effectiveness.

5.2 Recommendations

Based on the findings of this thesis, the author proposes several recommendations for organizations:

1. Automation and Clear Guidelines Are Key: While maturity assessments provide considerable benefits, they can delay releases if conducted manually. Streamlining these processes through automation and supplying clear remediation guidelines significantly reduces turnaround times and ensures that developers know exactly how to address identified issues.

2. Ongoing Improvements Are Essential: The DevSecOps lifecycle is continuous. Regularly revisiting and updating security practices based on new threats, feedback, and lessons learned ensures long-term resilience and alignment with evolving regulations and industry standards.

5.3 Future Works

Future research, could be further refined and enhanced through the following improvements:

1. Automate the security maturity process to minimize time overhead while ensuring applications achieve the required maturity level before production. Additionally, develop documentation and guidelines to standardize the maturity checklist.
2. Develop automated proactive monitoring solutions that integrate threat intelligence and multiple scanning tools, enabling security teams to quickly detect and address potential vulnerabilities with minimal manual effort.
3. Expand the maturity assessment checklist to address multiple compliance requirements, rather than focusing solely on a single standard. Encompass governance, auditing, and high-level compliance monitoring to ensure regulatory alignment and strategic oversight.
4. Benchmark security levels against companies with similar business models to ensure relevance in today's landscape.