EAT40005 Research Topics

Topic: Vulnerability Management

The rapid evolution of technology has led to faster software development cycles and frequent releases of new products. While this accelerates innovation, it also introduces significant security risks. Vulnerabilities in applications and infrastructure can expose organisations to cyberattacks, data breaches, and financial losses. Effective vulnerability management—identifying, assessing, and mitigating security weaknesses—has become crucial for mature technical teams. This report examines key strategies, tools, and best practices to manage modern software development and infrastructure vulnerabilities.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: Identify the most effective vulnerability management process in the Development Operations (DevOps) CI/CD pipeline.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should include,

1. Compare three vulnerability management solutions (AI-powered and traditional) across small to large tech teams, analysing their effectiveness for different organisational contexts and how key DevOps stakeholders (developers, SecOps, leadership) influence implementation approaches. The comparison should consider various key stakeholders involved in the DevOps process.
2. Evaluate the ethical (data privacy), economic (resource allocation), and technical (pipeline integration) challenges of these solutions against three NIST CSF maturity levels (Partial, Risk-Informed, and Repeatable), detailing optimal approaches for each maturity stage.
3. Predict how AI/automation will transform vulnerability management within 3-5 years across all maturity levels, enabling:
    a. Proactive threat detection scaled to team size
    b. Adaptive security postures for evolving DevOps pipelines
    c. Automated compliance with minimal workflow disruption

Topic: Source Code Review

As software development accelerates, secure coding practices have become critical to prevent vulnerabilities that could lead to data breaches, system compromises, or compliance failures. Source code reviews the systematic examination of code for security flaws—which is now a fundamental practice for mature technical teams. This report analyses how modern tools and methodologies can enhance code review processes while addressing implementation challenges.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: Identify the most effective source code review process in the Development Operations (DevOps) CI/CD pipeline by describing feasible approaches to introducing source code review into an agile DevOps CI/CD pipeline for three different NIST CSF Maturity Model maturity levels.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should include,

1. Compare implementation approaches for source code review across small to large tech teams, analysing how different DevOps stakeholders (developers, security teams, ops) influence integration strategies.
2. Evaluate solutions against three NIST CSF maturity levels (Partial, Risk-Informed, Repeatable), identifying appropriate tools and processes for each stage of organisational growth.
3. Predict how AI-powered code review will evolve to support all maturity levels, enabling automated compliance while adapting to team size and workflow differences.

Topic: How to Reduce Attack Surface

The recent pandemic has accelerated the advancement of technology at exponential rates. The need to access enterprise systems remotely arose overnight. A few years have passed, and most businesses are now operating entirely in the cloud or heading in that direction. This has introduced new variants of security vulnerabilities, including new attack vectors and enlarged attack surfaces. Attack surface refers to the potential entry points into an organisation, usually available externally on the Internet.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: Investigate methods to reduce organisational attack surface to reduce organisational threats.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should include,

1. Compare attack surface reduction methods across organisations of varying sizes of an average Australian business, analysing how key stakeholders (security teams, IT leadership, and employees) influence implementation strategies in hybrid work environments.
2. Evaluate solutions against three implementation maturity levels (Reactive/Basic, Proactive/Intermediate, Predictive/Advanced), identifying appropriate security controls and processes for each stage of security posture improvement. Detail the strengths and weaknesses of each of your documented methods. Provide publicly known examples where these methods have successfully reduced the impact of a breach or compromise.
3. Provide your recommendations of attack surface reduction method(s) for organizations to follow.

Topic: Threat Modeling

With the increase of media exposure and governance requirements within Australia in cybersecurity, organisations must make informed decisions on the best investment and approaches in cybersecurity.

Threat modelling allows businesses to quickly identify organisational or system-level threats within their context to identify the most relevant security controls without committing to significant investments initially.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: Compare all industry-recognised threat modelling frameworks.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should include,

1. Compare three threat modelling frameworks (e.g., STRIDE, PASTA, OCTAVE) by cost, time, and skill requirements, aligning each to organisational maturity (SMB to enterprise) and key stakeholder needs (technical teams vs. executives).
2. Analyse strengths/weaknesses per framework (e.g., STRIDE's developer agility vs. PASTA's governance depth), using Australian case examples (e.g., APRA CPS 234 compliance) to illustrate real-world applicability.
3. Predict emerging trends, such as AI-assisted threat modelling or Essential Eight-integrated tools, that could reduce barriers for Australian businesses.

Topic: AI tutors

Artificial Intelligence (AI) tutors are digital tools that use machine learning, NLP, and data analytics to assist students in their learning process. They offer personalised learning experiences, instant feedback, and 24/7 support, making education more engaging and efficient. AI tutors can assist in various subjects, adapt to individual learning styles, and help educators by automating repetitive tasks, allowing them to focus on higher-level teaching strategies.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: To explore how AI-powered tutors can improve student learning and teaching effectiveness by providing personalised, adaptive, and accessible educational support.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should include,

1. Identify and compare three AI-powered tutoring platforms' unique features and offerings in the context of personalised learning and teaching support.
2. Discuss the ethical, economic, and technical implications of relying on AI tutors in education.
3. Present an opinion/prediction on how these AI tutoring platforms may impact the current and future education landscape.

Topic: Accessibility with AI-powered Education Tools

Artificial Intelligence (AI) has the potential to revolutionise education by providing personalised and adaptive learning experiences. However, accessibility remains a significant challenge—many students, especially those from underprivileged backgrounds, face barriers such as lack of internet access, high costs, or disabilities that limit their ability to benefit from AI-powered learning tools. This report explores how AI can be made more inclusive, ensuring that every student can leverage these advancements regardless of socioeconomic status, location, or physical ability.

In this task, students are expected to conduct a literature review and write a research report on the above topic.

Objective: To investigate how AI-powered educational tools can be universally accessible to students regardless of their background, geographical location, or physical constraints while maintaining educational quality and effectiveness.

Description: Students need to present an analysis that synthesises literature, includes predictive insights/opinions about the topic, and justifies those with facts extracted from the literature review.

The report should:

1. Identify and compare three AI-powered educational tools designed to improve accessibility for students from diverse backgrounds and constraints.
2. Discuss the ethical, economic, and technical challenges in making AI tools universally accessible in education.
3. Present an opinion/prediction on how AI can bridge the accessibility gap in education in the future.