Dear Jane,
Thank you for agreeing to participate in my MSc dissertation research at University of Southwales, which develops a Python-based anomaly-based intrusion detectionsystem (IDS) for detecting Denial of Service (DoS) attacks using the NSL-KDD dataset.I appreciate your willingness to share your expertise via email, as a Zoom interviewwasn't feasible.

Purpose of the Study

This project evaluates my IDS software artefact by gathering general insights fromcybersecurity professionals on IDS functionality, usage, importance, risks, andchallenges, as well as perspectives on anomaly-based IDS and dataset relevance (e.g.,NSL-KDD vs. CICIDS-2017). Your email responses will help contextualize my researchand enhance artefact evaluation.

Consent Confirmation

You've received a consent form outlining the study's purpose, anonymity, data use, andstorage in a VeraCrypt-encrypted container (as my laptop lacks full-disk

encryption). Byresponding to this email, please confirm: “I consent to participate in this email interview,understand the terms in the provided consent form, and agree to anonymized use of myresponses. Contact me at 30133368@students.southwales.ac.uk with any questionsor to withdraw.

Interview Questions

Below are 12 questions about your general experiences with IDS, designed to take 15–20 minutes to answer. Please reply by 3rd July 2025, numbering your responses 1–12.No company-specific or sensitive information is needed, and responses will beanonymized (e.g., Participant 1) in my dissertation (Appendix X) to comply with GDPR.

- Can you describe your general experience with managing or using intrusiondetection systems in a professional cybersecurity environment?

- How are IDS typically deployed in workplace networks to monitor and protectagainst cyber threats?
- What role do IDS play in the overall cybersecurity strategy of an organization, andhow important are they compared to other security tools?
- What are the primary operational challenges you've encountered when using IDS inthe workplace, particularly in dynamic or high-traffic networks?
- In your experience, what are the most significant risks associated with relying onIDS for threat detection in professional settings?
- How do false positive alerts from IDS impact security operations, and whatstrategies have you seen used to manage them effectively?
- How do IDS integrate with other security systems, such as Intrusion PreventionSystems (IPS), Security Information and Event Management (SIEM), or SecurityOrchestration, Automation, and Response (SOAR)

platforms, in your workplaceexperience?

- What factors influence the choice between anomaly-based and signature-basedIDS in workplace cybersecurity strategies?
- How do organizations evaluate the effectiveness of IDS in the workplace, and whatmetrics or criteria are most valued?
- What are your thoughts on the effectiveness of anomaly-based IDS for detectingmodern threats, such as Denial of Service attacks, compared to traditionalapproaches?
- In your experience, how suitable are older datasets like NSL-KDD for developing orevaluating IDS, compared to newer datasets like CICIDS-2017?
- If an anomaly-based IDS for DoS detection achieves high accuracy and a low falsepositive rate, what considerations would you prioritize for its practical deployment ina workplace setting?

Instructions

- Reply to this email with your answers, numbered 1–12, at your convenience.
- Provide as much detail as you're comfortable with, or skip any questions.
- Avoid personal or company-specific details (e.g., company names, specificsystems) to ensure anonymity.
- If you haven't returned the signed consent form, please feel free to attach it orconfirm consent in your reply.

Data Handling

Your responses will be stored in a VeraCrypt-encrypted container, accessible only to me(and my supervisor, if required), and deleted after dissertation assessment (September 2025). Anonymized findings will appear in my Discussion and Appendix X, e.g.,"Participants noted false positive challenges (Participant 1, Appendix X)." For GDPRrights (e.g., access, deletion), contact me at 30133368@students.southwales.ac.uk.

Next

I’ll confirm receipt of your responses .Thank you for contributing to my research!
Best regards,
Afolalu Ayokunle MSc Student, University of Southwales
30133368@students.southwales.ac.uk