##Recommended Follow-up Actions

1. Conduct further research on Innovatech Solutions to gather more information about their infrastructure, technology stack, and organizational structure. This can be done through OSINT techniques such as searching for company profiles on professional networking sites, analyzing public job postings, and monitoring social media accounts.

2. Identify potential attack vectors and vulnerabilities based on the gathered information. This includes researching known vulnerabilities related to Rust programming language, Linux systems, RabbitMQ messaging systems, and microservices. This will help in identifying potential targets for exploitation during the penetration test.

3. Perform social engineering attacks targeting employees, especially new hires or less experienced staff. This can be done by researching employees' social media profiles, identifying their interests and personal information, and using this information to craft convincing phishing emails or targeted social engineering attacks. This will help in testing the company's security awareness and response to social engineering attacks.

4. Conduct penetration testing on the company's infrastructure, focusing on areas identified as potential vulnerabilities based on the gathered information. This includes testing for vulnerabilities in the Rust programming language, Linux systems, RabbitMQ messaging systems, and microservices. Additionally, test the effectiveness of the company's network security measures and the security of their OT systems.

5. Provide recommendations for improving the company's security posture based on the findings of the penetration test. This includes suggesting patches or updates for known vulnerabilities, recommending security best practices for the company's programming and networking practices, and suggesting improvements to the company's network security measures.

6. Continuously monitor the company's online presence and job postings for any new information that may be relevant to the penetration test. This includes regularly monitoring the company's social media accounts, job postings, and any public announcements or press releases. This will help in staying up-to-date with any changes in the company's infrastructure, technology stack, or organizational structure that may affect the penetration test.