Chris Hopkins

July 1, 2024

CYSE368

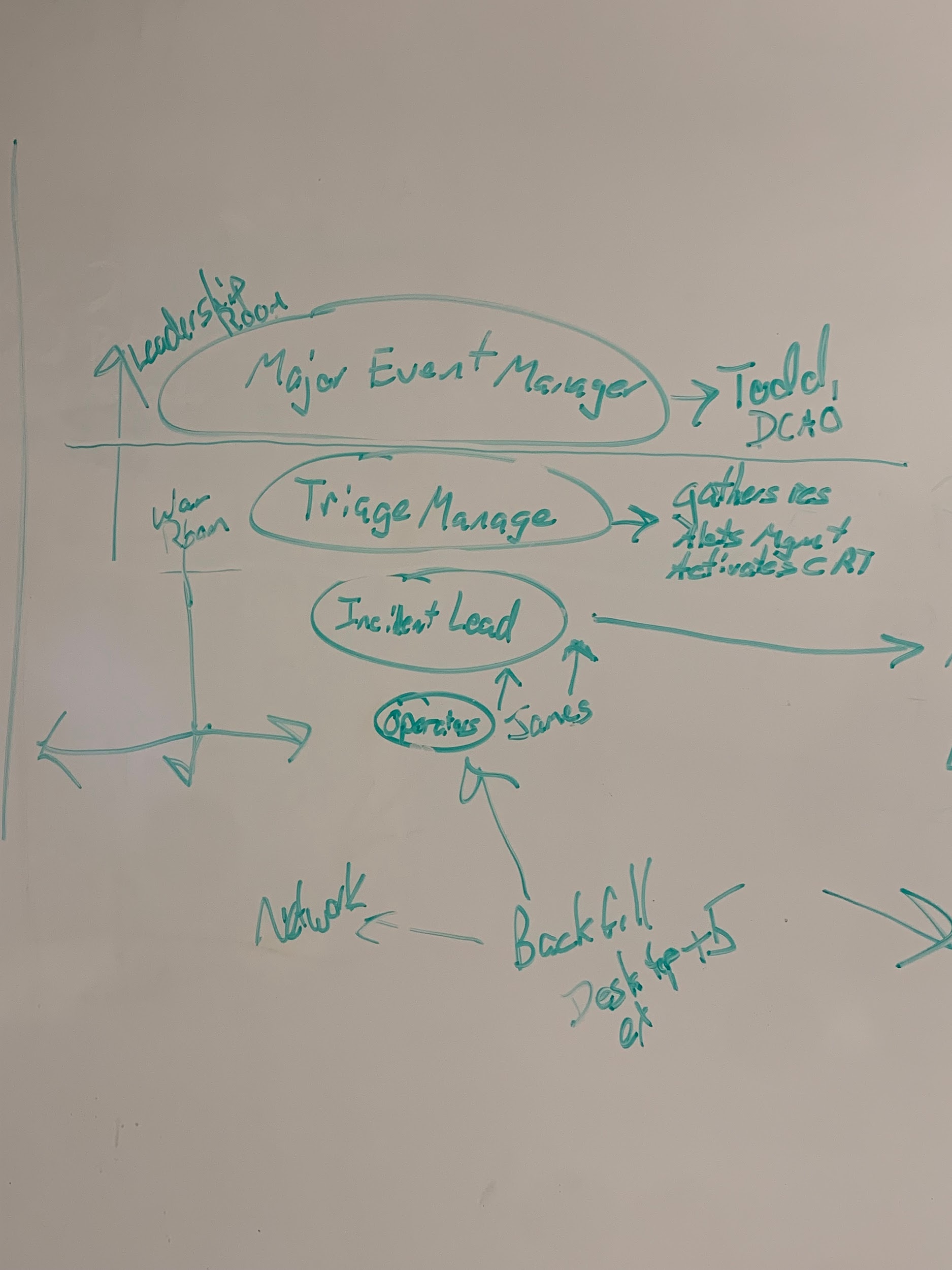
Reflection Paper 6

This week, I took part in the ongoing development of the Red Book, a crucial component of our incident response plan. The meeting, led by my supervisor Douglas Gernat, focused on refining the roles, scope, and chain of command necessary for an effective incident response. Our goal was to ensure that every team member understands their responsibilities and the overall structure of the response strategy.

We began by defining the key roles within the incident response team. These roles include the operator, the initial responder to an incident; the incident lead, who coordinates all response activities; the triage manager, responsible for prioritizing incidents based on their severity and potential impact; and the major event manager, who oversees the handling of significant incidents that affect multiple systems or stakeholders. Clarifying these roles is essential for maintaining an organized and efficient response during a crisis. The meeting also addressed peripheral aspects of the incident response plan. This included the role of the Office of Security Management, which ensures the overall security and preparedness of the organization. We discussed the importance of vendor distribution, emphasizing the need for strong relationships with external vendors to secure timely support and resources during an incident. Another critical topic was the concept of fusion, a strategy used to rally additional personnel when threats exceed the capacity of our current response team. This approach is vital for scaling our efforts and ensuring that we have enough resources to handle extensive threats effectively.

This collaborative session was key to improving the Red Book and strengthening our incident response plan. By clearly defining roles and addressing additional strategic elements, we aim to build a robust and effective incident response framework. This experience has significantly enhanced my understanding of incident management and highlighted the importance of thorough planning and clear communication in ensuring a rapid and effective response to security incidents.

Photos of Hunt & Incident Response Team Coin and Response Plan Role Scope:



**Referenced Works**

Legitt. "FIDIC Red Book: Comprehensive Guide to Construction Contracts." *Legitt AI*, 19 July 2023,<https://legittai.com/blog/guide-to-fidic-red-book-contracts>. Accessed 2 July 2024.