**EAS 596 – CYBERSECURITY ANALYTICS**

**CRITICAL RESPONSE 3**

Overall, this course was highly valuable and provided a strong foundation for understanding how **Security Information and Event Management (SIEM)** systems function. It effectively covered key concepts and offered practical exposure to working with SIEM tools, which significantly enhanced my learning experience.

One of the most impactful aspects of the course was the **final project**. It offered a hands-on, real-world simulation that allowed me to apply what I had learned in a meaningful way. Working with Splunk during the project deepened my understanding of log analysis, threat detection, and incident correlation. It was not only educational but also an exciting opportunity to gain experience with an industry-standard tool.

However, I would like to offer a suggestion for improvement. The session that covered **metrics and the pragmatic approach** felt a little dense. It attempted to cover a large amount of information in a single lecture, which made it challenging to absorb everything effectively. Splitting this topic into two separate sessions would make the content easier and enhance understanding.

Aside from that, the course was well-structured and thoughtfully designed. The combination of theoretical lessons with practical application made it engaging and comprehensive. I walked away from this course with a much clearer understanding of how SIEM tools are used in real-world environments, and I feel more confident in applying these concepts moving forward.