**회의록**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 회의일시 | 2021년 05월 24일 | 팀명 | 이벤트샵 | 작성자 | 김한진 |
| 참석자 | 김한진, 공경선, 금소영, 김동관, 김범, 서용석, 최병섭 | | | | |

|  |  |
| --- | --- |
| 회의안건 | **1. 중간발표 피드백 정리**  **2. 클라우드 계획서 수정** |

|  |  |  |
| --- | --- | --- |
| 회의내용 | 내용 | 이슈 / 비고 |
| **1. 중간발표 피드백 정리**  **1) 질문**  **- 1. 질문 : azure 서비스가 싱가폴도 있는 데 왜 호주만 사용하는 가?**  **- 2. 질문 : 계정 관리는 aws에서 하는 가? azure에서 하는 가?**  **- 3. 질문 : 웹 서비스에 대한 공격 로그를 lambda에서 s3에 저장되는 거 지금 되고 있나?**  **- 4. 질문 : 컨설팅이에요, 구축이에요? 정확히 무엇인가?**  **- 5. 질문 : 마이그레이션을 할 때 되는 게 있고 안되는게 있는 데 그런 부분에 대한 고려한 부분은 없다!**  **- 6. 질문 : 일, 월별로 생성된 문서는 어떻게 보여줄 것 인가?**  **- 7. SIEM을 구현하겠다는 것인데 이 것은 보고서로만 발행식만으로만 보여주는 것인가?**  **- 8. 질문 : 이 제품을 고객들이 살 이유는 무엇인가? -> ( 한진이가 대답한 내용을 잘 정리해서 최종 때 발표하면 좋을 것 같다고 멘토님이 말씀하심! )**  **- 9. 질문 : SIEM인데 기존의 SIEM 제품들과 차별점이 무엇이 있는 지, 그 차별점이 무엇인 지 중점으로 발표하면 좋을 것 같다.**  **- 10. 질문 : 이 제품을 써야 하는 당위서(보고서)를 만들면 좋겠다. 발표할 때 람다에 대한 코드 관련 부분은 보고 싶지 않다.**  **- 11. 질문 : 혹시 저장공간에 대해서 로그와 보고서를 저장하는 데 이 용량에 대한 비용을 생각해본적이 있나? 이 비용이 어마어마하게 나올 수도 있다.**  **- 12. 질문 : 비정상적인 이벤트에 대해 어떻게 판단할 수 있을 까? 이 것이 명확하게 나오면 제품 살 것 같다!**  **2)피드백**  **- 에져 센티얼은 사고가 날 때 로그가 기록을 하고 그런 기록을 상관분석등을 통해 분석을 하는 것인가?**  **- SIEM을 구축한다는 말을 들으면 엄청 큰 통합 시스템을 만드는 것으로 들리는 데 막상 결과물을 보면 보고서 만들기 등으로 기본적인 시스템을 구축하는 것으로 보이기 때문에 SIEM이라고 말하기 어려운 것 같다.**  **- 일반적으로 멀티 클라우드라고 하면 양쪽 클라우드에 동일한 시스템을 구성한 것으로 생각했었다. 근데 발표한 아키텍처를 보니 멀티 클라우드라기 보다는 하이브리드 클라우드에 가까운 것 같다.**  **- 현장에서는 로그 자체를 수집할 때 로그 파일 사이즈가 너무 크다 보니 클라우드 S3에 저장하는 데 고민이 되었다. 그래서 S3는 로컬 에다가 저장하고 분석을 클라우드 에서 하고 있는 방향으로 진행되고 있다.**  **- 파일 스토리지? 는 비용이 많이 들지 않는 다. -> ( 멘토님 이 말하는 부분인데 정확히 못 적음 -> 우리 멘토님이 충고하신 부분이니 추후에 다시 물어볼 것! )**  **- 트래픽에 대해 돈이 많이 들어간다. 그래서 최대한 필요한 데이터만 필터링하고 여기서 어떤 데이터가 필요한 데이터인지 기준을 정해야 한다** |  |
| **2. 클라우드 계획서 수정**  - 클라우드 계획서 수정하여 Azure 바우처 신청 |  |

|  |  |  |
| --- | --- | --- |
| 결정사항 | 내용 | 진행일정 |
| 중간발표 피드백 정리 | 2021-05-24 |
| 클라우드 계획서 수정 | 2021-05-24 |
|  |  |