<주요 Q&A>

클라우드 보안 FAQ
- 10년 동안 클라우드 보안에 대해 가장 많이 받은 질문들

Q1. 클라우드를 처음 도입하고자 하는 입장에서, 어떠한 사업자를 선정해야 하는지에 대한 고민도 있는데요, 나에게 적합한 클라우드 사업자 선정을 위한 특별한 기준 같은 것이 있을까요?

처음 클라우드 전환을 고려하신다면 최대한 Major CSP를 고려하시는 것이 좋습니다. Minor CSP가 비용 경쟁력이 있어도 인력과 학습비용을 고려해야 하기 때문입니다. CSP의 보안은 보안 기능뿐 아니라 이를 보조하는 관리, 모니터링 같은 기능도 중요합니다.

Q2. 클라우드 보안 취약점 체크리스트가 공개된 자료가 있나요?

클라우드 보아 체크리스트는 CSP와 플랫폼 별로 공개된 버전이 있습니다. 주로 CIS (Center for Internet Security)의 것을 자주 사용합니다. AWS/Azure/GCP/AliCloud/IBM과 Docker/K8s/Openshift 등이 있습니다. 클라우드 보안 체크리스트는 CSP와 플랫폼 별로 공개된 버전이 있습니다. 주로 CIS (Center for Internet Security)의 것을 자주 사용합니다. AWS/Azure/GCP/AliCloud/IBM과 Docker/K8s/Openshift 등이 있습니다.

Q3. 고객-MSP-MSPP 삼각구도의 운영방식에 대하여 삼성SDS가 제공하거나 서비스하는 내용이 있나요?

네, 저희 보안진단 서비스 중에는 클라우드에 대한 진단 이외에도 클라우드를 운영하는 사람에 대한 진단도 겸하고 있습니다. 운영자의 보안 위규와 위규 이후의 작업 이력 등을 종합적으로 진단합니다.

Q4. 멀티클라우드를 사용하는 경우 보안과 관련하여 특별히 더 신경 써야 하는 부분이 있을까요?

각 CSP마다의 보안 컨셉은 유사하나 구성 방식과 설정 방법이 달라 관리에 어려움이 있을 수 있습니다. 별도의 솔루션 없이 각각 관리한다면 보안성의 유지에 어려움이 있을 수 있어 Managed 서비스를 사용하는 것을 권장 드립니다.