진단 대상	진단 항목	답변 예시
클라우드 관리 콘솔 (AWS)	CloudFront 접근 통제	**비인가자의 내부 네트워크 접근으로 인한 정보 유출 등 침해 사고 발생을 통제하고 있는가?** **1) IAM Role/Policy 기반** 점검 경로 : IAM > 액세스 관리 > 정책 > 글로벌 서비스 답변예시) 리전이 설정되어 있으며, 담당자 OOO이 월간 점검을 통해 설정 변경 여부를 AWS 통합 점검 파일에 기록하고 있음 **2) Access log활성화 사항** 점검 경로 : CloudFront > 원격 측정 > 로그 > 스탠더드 답변예시) 로그 파일을 생성하도록 CloudFront를 구성하여 '표준 로그'가 '활성화됨', '실시간 로그'가 '사용 중지'로 설정하고 있으며 담당자 OOO이 월간 점검을 통해 설정 변경 여부를 AWS 통합 점검 파일에 기록하고 있음
클라우드 관리 콘솔 (AWS)	VPC Endpoin Service 접근 통제	**VPC Endpoint Service 접근 통제하여 비인가된 외부 VPC에서 연결 요청하지 못하도록 "수동 연결" 설정하고 있는가?** **1) VPC Endpoint Service의 수동 연결 설정 여부 확인** 점검 경로 : 리전별 VPC > 가상 프라이빗 클라우드 > 엔드포인트 서비스 > 서비스 이름 답변예시) 서비스 목록 존재를 확인할 수 있으며 담당자 OOO이 월간 점검을 통해 설정 변경 여부를 AWS 통합 점검 파일에 기록하고 있음 **2) VPC Endpoint Service 생성 케이스** 점검 경로 : VPC > 가상 프라이빗 클라우드 > 엔드포인트 서비스 > 엔드포인트 서비스 생성 > 추가 설정 > 세부 정보 답변예시) "수락 필수"를 "아니오"로 설정하여 외부에서 들어오는 엔드포인트를 차단하고 있으며 담당자 OOO이 월간 점검을 통해 설정 변경 여부를 AWS 통합 점검 파일에 기록하고 있음
클라우드 관리 콘솔 (AWS)	이미지 취약점 점검	**이미지 취약점 점검 시 골든 이미지 하드닝 절차를 따르고 있는가?** **1) AMI(OS) 이미지** 답변예시) Build 시 OS 자체 스크립트 이용하여 점검하고 있으며 시스템 보안팀이 월간 점검 보고서를 작성하고 있음 **2) Docker 이미지** 답변예시) 시스템 보안팀이 관리하고 있으며 월간 점검 보고서를 작성하고 있음
클라우드 관리 콘솔 (AWS)	승인된 이미지만 배포	**승인된 AMI만 EC2 인스턴스로 배포하고 있는가?** 점검 경로 : EC2 > 이미지 > AMI 답변예시) EC2, EKS에 실제 배포된 AMI 목록과 전산상 AMI 목록이 일치하고 있으며 담당자 OOO이 AWS 통합 점검 파일의 AMI 시트에 EC2와 EKS의 AMI 목록을 정리하여 일치 여부를 매월 관리하고 있음
클라우드 관리 콘솔 (AWS)	클라우드 자원간 접근 시에는 임시 자격증명 사용	**클라우드 자원간 접근 시에는 임시 자격증명을 사용하고 있는가?** 답변예시) AWS STS(Security Token Service)를 통해 발급되는 임시 보안 자격증명 AWS:STS:AssumedRole에 리소스명 biz-sec-apne2-hawkeye-trail_data-etl_lambda로 사용하고 있음
클라우드 관리 콘솔 (AWS)	Access Key 코드에 직접 삽입 금지	**Access Key의 삽입을 제한하여 관리하고 있는가?** 답변예시) 임시 보안 자격증명을 사용하고 있으므로 Access Key 삽입을 제한하고 있음
클라우드 관리 콘솔 (AWS)	Access Key 90일마다 변경	**Access Key의 자격 증명 유효기간을 최대 90일로 설정하고 있는가?** 점검 경로 : IAM > 액세스 관리 > 사용자 > 사용자명 > 보안 자격 증명 > 액세스 키 답변예시) "생성 완료" 설정이 "90일" 이내로 설정되어 있음
클라우드 관리 콘솔 (AWS)	계정 인증에 대해 타임아웃 30분 적용	**1) AWS 계정 인증에 대한 세션 타임아웃을 30분 이내로 적용하고 있는가?** 점검 경로 : IAM Identity Center > 권한 세트 > 세션 기간 답변예시) "30분"으로 설정되어 있음 **2) SSO 이용하여 관리자에 의해 정기적으로 계정별 세션 확인하고 있는가?** 답변예시) Keycloak 연동하여 로그인 수행하고 있으며 자사 보안관제센터에 의해 매시간 계정별 세션 확인하고 있음
클라우드 관리 콘솔 (AWS)	허용된 계정만 콘솔에 접근할 수 있도록 통제	**1) AWS 접근제어시스템에서 사전에 허용된 계정만 콘솔에 접근할 수 있도록 설정 관리하고 있는가?** 점검 경로 : IAM Identity Center > AWS 계정 > 조직 구조 답변예시) 각 조직 단위에 속한 사용자 이름을 확인 후 주기적으로 월간 접속로그 보고서 작성하여 접근 통제 내역 관리하고 있음 **2) 접속인증시스템 기능을 통해 허용된 계정만 접속할 수 있도록 관리하고 있는가?** 답변예시) 외부 SSO 기능 Keycloak을 통해 계정별 권한 설정하여 접근 제어하고 있음
클라우드 관리 콘솔 (AWS)	접근 가능 단말기 IP 지정	**클라우드서비스 계정에 대한 접근 가능 단말기 IP 지정하고 있는가?** Proxy 접근 단말기 답변예시) 클라우드서비스 프로비저닝 VDI로 제한하고 있음

클라우드 관리콘솔(Azure) 질의서

진단 대상	진단 항목	답변 예시
클라우드 관리콘솔 (Azure)	초기 비밀번호 변경	**초기 비밀번호를 변경하여 사용하고 있는가?** 점검 경로 : Azure > 사용자 생성 > "임시 비밀번호 생성" & "사용자 지정 비밀번호" 답변예시) 최초 로그인 시에 비밀번호 업데이트하도록 정책 설정하고 있음
클라우드 관리콘솔 (Azure)	비밀번호 변경 시 동일한 비밀번호 설정 제한	**비밀번호 변경 시 이전에 사용한 동일한 비밀번호 사용 제한 설정을 하고 있는가?** 답변예시) 이전에 사용한 동일한 비밀번호 사용 제한 정책 설정하고 있음
클라우드 관리콘솔 (Azure)	분기별 1회 이상 비밀번호 변경	**패스워드 만료 기간이 90일로 설정되어 있는가?** 점검 경로 : Azure 기본 암호 정책 > 암호 만료 기간 답변예시) Azure 기본 암호 정책 "90일" 사용하고 있음
클라우드 관리콘솔 (Azure)	일방향 알고리즘으로 암호화 저장	**비밀번호를 일방향 알고리즘 (SHA256 이상)으로 암호화하여 저장하고 있는가?** **1) 표준 및 권장 암호화 알고리즘 사용** 답변예시) Azure 데이터 암호화에 SHA256 알고리즘 사용하고 있음 **2) 보안 해시 알고리즘(SHA-2 제품군) 사용** 답변예시) SHA-2 제품군만 사용하고 있음 **3) 추가 Key 사용 여부** 답변예시) KEK(키 암호화 키)를 DEK(데이터 암호화 키) 보호하기 위해 사용하고 있음
클라우드 관리콘솔 (Azure)	특성과 용도에 따라 구독 (Subscription) 분리	**관리그룹, 구독, 리소스 그룹이 용도에 맞게 분리되어 있는가?** 점검 경로 : 1) 관리 그룹 > '개요' 및 하위 구독, 리소스 현황 2) 구독 > 리소스 그룹 메뉴 현황 3) 리소스 그룹 > '개요' 및 리소스 그룹 정보 현황 답변 예시) 용도에 따라 관리그룹, 구독, 리소스 그룹으로 분리하고 있음
클라우드 관리콘솔 (Azure)	클라우드서비스 계정 접근 시 2-Factor 인증 수단 적용	**클라우드서비스 계정 접근 시 2-Factor 인증 수단을 적용하고 있는가?** 답변 예시) 클라우드 서비스에 접근하는 모든 계정에 MFA 적용하고 있음
클라우드 관리콘솔 (Azure)	계정 인증에 대해 타임아웃 30분 적용	**디렉터리 수준 유휴 시간 제한 사용 설정이 30분 이하로 적용되어 있는가?** 답변 예시) 디렉터리 수준 유휴 시간 제한 사용 설정이 30분으로 설정되어 있음

클라우드 관리체계 질의서

진단 대상	진단 항목	답변 예시
클라우드 관리체계	주기적으로 가상화 인스턴스(가상머신, 컨테이너) 식별 여부	**주기적으로 가상화 인스턴스 식별하고 있는가?** 답변예시) 자산 중요도 평가 파일에 가상화 인스턴스 자산 목록을 정기적으로 갱신하여 자산 중요도에 따라 자산 분류하여 관리하고 있음
클라우드 관리체계	가상화 인스턴스(가상머신, 컨테이너)의 생성, 변경, 회수 등에 관한 승인절차 수립 및 이행	**각 가상화 인스턴스의 생성, 변경, 회수 등 모든 과정 승인 절차를 수립하고 있는가?** 답변예시) **1) OS 가상화** ITSM (서비스 관리 프레임워크) 사용하여 ITSM 솔루션을 통해 가상화 인스턴스 승인 프로세스를 정형화하고 있음 **2) K8s Node** ITSM (서비스 관리 프레임워크) 사용하여 ITSM 솔루션을 통해 가상화 인스턴스 승인 프로세스를 정형화하고 있음 **3) K8s Container** Gitlab : 코드/배포 승인 관리하고 있음 ITSVC : 가상화 인스턴스 승인 프로세스를 정형화하고 있음
클라우드 관리체계	가상화 인스턴스(가상머신, 컨테이너) 변경에 대한 기록 관리	**각 가상화 인스턴스 변경 기록을 이력 내역 기록, 분기별 유효성 점검을 통해 관리하고 있는가?** **1) OS 가상화** ITSM을 통해 가상화 인스턴스 생성/변경/삭제에 대한 사전 결재 및 이력관리 수행, Pod 레벨의 변경사항에 대한 유효성 점검하고 있음 **2) K8s Node** ITSM을 통해 가상화 인스턴스 생성/변경/삭제에 대한 사전 결재 및 이력관리 수행, Pod 레벨의 변경사항에 대한 유효성 점검하고 있음 **3) K8s Container** ITSVC를 통해 가상화 인스턴스 생성/변경/삭제에 대한 사전 결재 및 이력관리 수행, Pod 레벨의 변경사항에 대한 유효성 점검하고 있음
클라우드 관리체계	가상화 인스턴스(가상머신, 컨테이너)의 보안 등급에 따른 책임자 지정	**자산 중요도 평가 파일을 통해 가상화 인스턴스를 식별하고 각 인스턴스에 책임자를 지정하고 있는가?** 답변예시) 자산 중요도 평가 파일에 각 가상화 인스턴스의 보안 등급별로 책임자 지정하여 관리하고 있음
클라우드 관리체계	가상머신 구축시 표준 이미지 미사용	**가상머신 구축 시 표준 이미지를 생성하여 사용하고 있는가?** **1) OS 가상화** 하드닝 스크립트 실행한 VM 스냅샷으로 표준 이미지 배포하고 있음 **2) K8s** 정보보안 OOO팀으로부터 받은 표준 이미지 점검하고 있음