

1. 서비스 오퍼링 | SecuXper

LG CNS SecuXper Cloud 서비스는 안전한 클라우드 전환/구축, 운영을 위한 보안 컨설팅, 시스템 구축, 솔루션 공급 및 보안 관제를 포함하는 토털 서비스입니다.

고객사에 최적화된 클라우드 정보보안 모델을 제시하여 선진 클라우드 정보보호 체계 마련

- 금융 클라우드 보안 컴플라이언스
- 클라우드 마이그레이션 보안체계 수립
- 클라우드 환경 ISMS-P 인증 등

내외부 발생하는 보안 위협에 대응하기 위한 클라우드 보안 시스템 설계 및 구축

- 클라우드 Native를 이용한 보안체계 구축
- 클라우드 전용 보안 솔루션 선정 및 구축 (CSPM / CWPP / CASB / ZTNA / SASE 등)



클라우드 환경에 대한 보안 설정을 점검하고 조치할 수 있는 자체 개발 솔루션 제공

- Azure 클라우드 보안 설정 점검
- 국내 개인정보보호법 등 컴플라이언스 기준

해킹/악성코드 등 외부 위협을 실시간 감지 및 대응할 수 있는 관제/운영 서비스

- 24 x 365 보안 관제 서비스
- 클라우드 Native 서비스 보안운영/관제
- 클라우드 전용 보안 솔루션 보안운영/관제 (CSPM / CWPP 등)

해킹·컴플라이언스 위반·개인정보 유출 등의 보안 리스크에 대응하여
고객사의 경영 및 재무적 손실을 최소화하기 위한 다양한 정보보안 컨설팅 서비스를 제공합니다.



Q. 클라우드 전환 시 보안은 어떻게 하나요?

A Transformation Consulting

- On-Premise 환경의 클라우드 전환 시, 보안 기술 설계 및 관리 정책 컨설팅
 - To-Be 보안 아키텍처 구성 전략
 - 클라우드 내 보안정책·기준·가이드 제시

Q. 클라우드 환경이 보안이 적절하게 반영 되었을까요?

A Technical Assessment

- 클라우드 전환된 환경에 대한 취약점 진단 서비스
 - LG그룹 클라우드 보안 가이드 기준
 - 접근제어, 계정관리, 권한설정 등 59개 점검항목에 대한 진단 및 개선방안 제시

Q. 클라우드 환경이 개인정보보호법/망법 준수가 되나요?

A Compliance Assessment

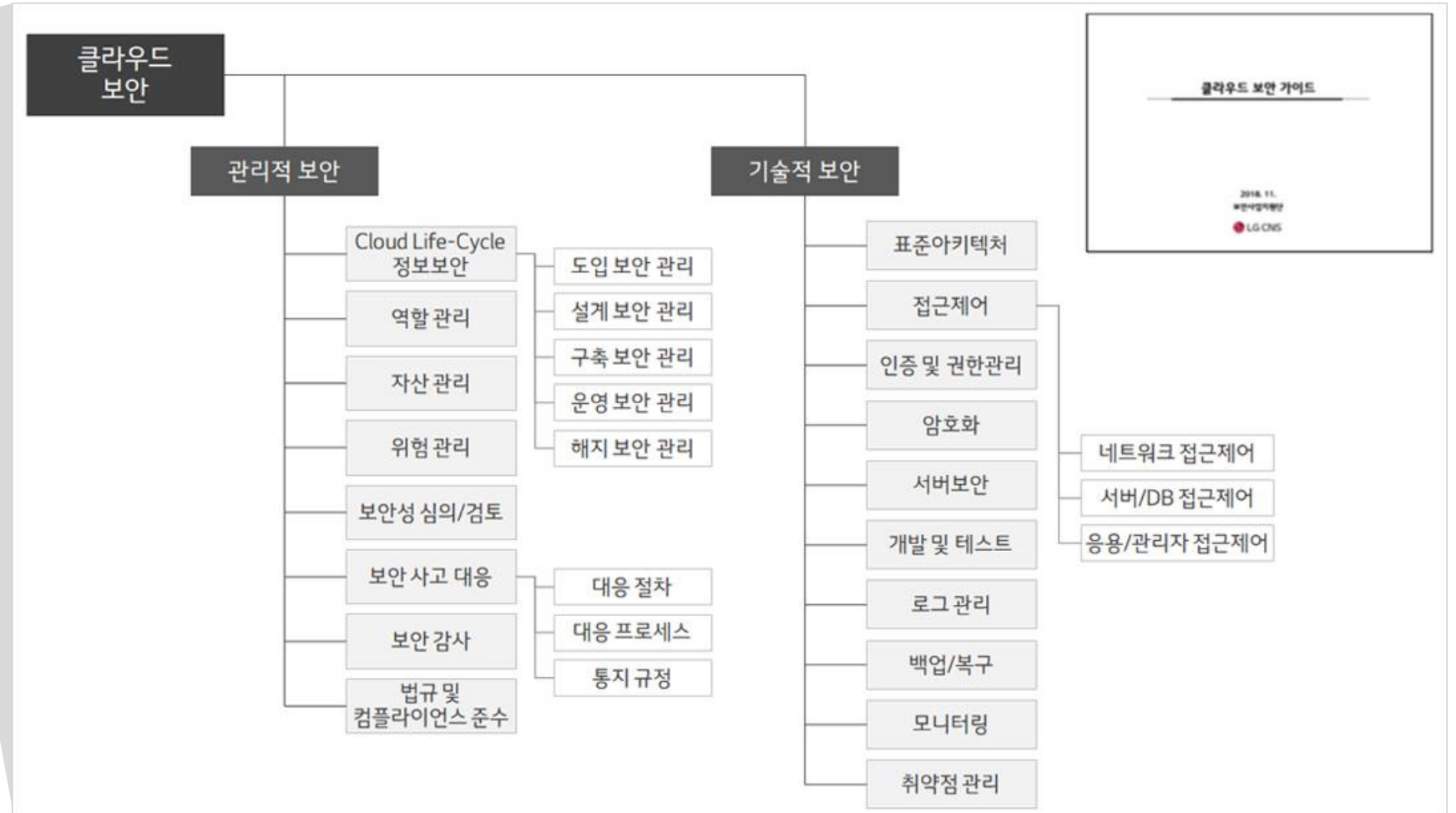
- 클라우드 환경에 대한 법적 준거성 진단
 - 개인정보보호법, 정보통신망법 등 보안관련 법률 기준
 - 법률 준수 현황 점검 및 대응방안 / 가이드 제시

Q. 클라우드 환경에서 ISMS-P 인증을 받고 싶습니다.

A Certification Consulting

- 클라우드 환경에 대한 금융보안원 보안인증, ISMS-P 인증 대응 컨설팅
 - 보안 인증 통제항목 기준
 - 보안 인증 획득을 위한 현황점검, 개선방안 제시, 심사 대응전략 수립

고객사에 최적화된 클라우드 정보보안 모델을 제시하여 선진 클라우드 정보보호 체계를 마련합니다.



고객사에 최적화된 클라우드 정보보안 모델을 제시하여 선진 클라우드 정보보호 체계를 마련합니다.



금융분야 클라우드 컴퓨팅서비스 이용가이드 구성

	01 사전준비	02 계약 체결	03 보고 및 이용	04 이용종료
개요	클라우드 이용을 위해 금융 감독기관이 정한 요건 충족 단계	클라우드 서비스 이용을 위한 계약 체결	금융회사의 클라우드 서비스 이용 위한 감독기관 보고 이행	출구 전략 이행
수행 내용	01 이용 대상 선정 및 중요도 평가	11 위수탁 계약서 관련 주요 컴플라이언스 요건 확인 <ul style="list-style-type: none"> 데이터 처리 위치, 훈련 및 취약점 분석 평가 등에 대한 협조, 위탁 업무의 이전·반환 등에 관한 사항 반영 금융당국 조사·접근 (현장방문 포함) 협조 의무 명시 	13 서류 구비 및 사전 보고 구비 <ul style="list-style-type: none"> 이용대상 및 중요도평가, 출구전략, 제공자 후보선정 및 평가 결과 등 	20 Exit 이행 <ul style="list-style-type: none"> 수립 Exit 진단결과 및 이행 계획기준 Exit 이행
	02 BCP 계획 수립		14 서류 최신성 유지 및 수시 보고체계 수립 <ul style="list-style-type: none"> 관리 방안 및 보고 계획 등 	
	03 안정성 확보 조치 방안 수립			
	04 업무위탁 운영 기준 마련			
	05 서비스 제공자 평가 및 선정			
	06 정보위원회 심의/의결			
수행 결과	07 중요도 평가 기준 및 결과서	12 금융회사 업무위탁 관한 규정 제7조 제 1항 각호 관한 서류 <ul style="list-style-type: none"> 위탁계약서, 업무 위수탁 운영기준, 준법감시인 검토 의견 위탁 필요성 및 기대효과 위탁 따른 업무 절차 변경 내용 	15 업무 위탁 규정 제7조 제1항 서류	21 Migration <ul style="list-style-type: none"> 클라우드서비스 제공자 전환
	08 클라우드 이용 관련 BCP 계획		16 중요도 평가 기준 및 결과서	
	09 안정성 확보 조치 사항 결과		17 클라우드 이용관련 BCP 계획서	
	10 정보보호위원회 심의/의결		18 안정성 확보 조치 사항 결과	

2. 서비스 오퍼링 | Implementation

다양한 산업군에서 풍부한 경험을 바탕으로 정립된 구축 절차와 품질, 사업관리 등 전문 지원조직과의 협업으로 고객사의 비즈니스에 최적화된 보안시스템을 설계하고 구축합니다.



Q. 어느 수준까지 보안 대책을 구현해야 하나요?

A 클라우드 보안 아키텍처 설계 및 구현

- '보안 책임 공유 모델'에 입각하여 안전한 클라우드 환경 설계 및 구축
 - On-Premise와 동등하거나 향상된 보호대책 설계 및 구현
 - 하이브리드 및 멀티 클라우드 환경의 보호대책 설계 및 구현

Q. 클라우드 전용 보안 솔루션은 없나요?

A Native 클라우드 보안 솔루션 선정

- 고객 환경에 적합한 검증된 클라우드 Native 보안 솔루션 제시
 - 신규 보안 솔루션 검증 완료 (CSPM, CASB, CWPP 등)
 - 서버리스, 컨테이너 등 최근 어플리케이션 아키텍처를 고려한 보안 대책 설계

Q. 클라우드의 장점을 최대한 활용하기 위한 설계는?

A Native 보안 기능 및 서비스 중점 구현

- CSP의 기본 보안 기능과 서비스를 최대한 활용한 설계 및 구현
 - Auto Scaling, 잦은 자원 변경 등 클라우드 환경에 적합한 보안 아키텍처 제시
 - 3rd Party 보안 솔루션을 최소화한 보호대책 구현

기능 계층	해킹/ 악성코드	접근제어	인증/ 권한관리	암호화	로그 및 모니터링	취약점관리	Compliance
어플리케이션	Azure WAF	SSO/IAM		SSL	WAS 모니터링	소스코드 진단	개인정보 영향평가
네트워크	Azure Firewall	Network Security Group	Azure AD		접속기록	모의해킹	
DBMS	Azure Defender	DB접근 제어		Key Vault	통합 보안관제	취약점 진단 (수작업)	
서버OS		서버접근 제어			Audit Logs / Security Center / Advanced Threat Protection / Sentinel	인프라 취약점 진단틀	
Cloud 환경/설정	Azure Security Center	웹콘솔(MFA) CLI (엑세스키)				클라우드 취약점 진단틀	
LG CNS 클라우드 보안 프레임워크 (Azure)		3rd Party	Azure Native	LG CNS 서비스/점검틀	보안 기술	규제/ Compliance	

2. 서비스 오퍼링 | Implementation

클라우드 환경도 기존 On-Premise 환경과 유사하게 전체 보안 아키텍처 관점에서 접근해야 합니다.



계층 \ 기능	해킹/악성코드	접근제어	인증/권한관리	암호화	로깅 및 모니터링	취약점관리	Compliance
어플리케이션	Azure WAF	SSO/IAM			WAS 모니터링 접속기록	소스코드 진단 모의해킹	개인정보 영향평가
네트워크	Azure Firewall	Security Group NACL		SSL	통합 보안관제	취약점 진단 (수작업)	기업 보안표준 국내외 법규(전자정보보호법, 개인정보보호법, 신용정보법)
<i>SAMPLE</i>							
DBMS	Azure Defender	DB접근 제어	Azure AD	Key Vault	Audit Logs / Security Center / Advanced Threat Protection / Sentinel	인프라 취약점 진단들	
서버OS		서버접근 제어					
Cloud 환경/설정	Azure Security Center	웹콘솔(MFA) CLI (엑세스키)				클라우드 취약점 진단들	
LG CNS 클라우드 보안 프레임워크 (Azure)		3rd Party	Azure Native	LG CNS 서비스/점검들	보안기술	규제/Compliance	

Native 보안 서비스 우선 적용

- 최소한의 클라우드 보안통제를 위한 기본 Baseline 설정
- 필수 보안기능 활성화 (예: Audit Logs)
- 글로벌 클라우드 서비스 제공자의 Threat Intelligence를 최대한 활용할 수 있는 Native 보안 서비스 적용 (예: Security Center, Sentinel)

3rd Party 솔루션은 반드시 검증

- 국내 컴플라이언스 요건을 충족하기 위해서는 3rd Party 보안 솔루션이 필요하므로 도입 전 반드시 적용 가능성 검증
- VM 위에 설치 가능한 소프트웨어 방식 솔루션인가?
- 수시로 변경되는 IP가 아닌 도메인 기반 통제가 가능한가?
- Auto Scaling 등 자원 변화에 유연하게 대응할 수 있는가?

고객사에서 운영 중인 클라우드 서비스의 보안 취약점을 통합 점검하여 해결방안을 제시하고 점검 이력을 관리하여 보안 수준을 상향 유지하기 위한 자동화 도구를 제공합니다.



Q. 수많은 가상자원과 서비스를 일일이 검사해야 하나요?

A One-Click Diagnosis

- 클라우드 보안설정 취약점 진단 자동화
 - 멀티 클라우드 보안설정에서 발생하는 취약점을 한 번 클릭으로 점검 및 자동 조치

Q. 국내법 요건에 부합하는 설정인지 확인할 수는 없나요?

A Compliance Check

- 국내 컴플라이언스와 연계된 점검항목 도출
 - 구성된 클라우드 환경의 국내법 기술적 보호조치 준수 여부 확인

Q. 발견된 취약점은 어떻게 조치해야 하나요?

A Comprehensive Reports

- 점검 결과를 Excel 형태 보고서로 제공
 - 취약점 발견 시 관련 법률 및 세부 조치 방법을 안내하는 보고서 제공

Q. 취약한 설정이 없는지 대해 한 눈에 확인할 수는 없나요?

A One-Click Dashboard

- 양호/취약 계정 등의 Dashboard 제공
 - 대시보드에서 점검 대상 서비스/프로젝트 별 보안 점검 결과, 양호/취약 계정 및 이력을 한 눈에 확인

2. 서비스 오퍼링 | Solution

LG CNS의 'CAT(Cloud Assessment Tool)'을 활용하여 클라우드의 보안 설정을 점검하고 조치합니다.



No	프로젝트 ID	프로젝트 명	담당자	CSP	취득 일자	점검 결과
11	PRJ20200906000001	테스트	김민준	Azure	2020/09/06 11:46:35	100
12	PRJ20200916000002	테스트	김민준	Azure	2020/09/16 14:42:32	100
13	PRJ20201030000003	테스트	김민준	Azure	2020/10/30 14:25:41	100
14	PRJ20201106000004	실용 - 고객사	김민준	Azure	2020/11/06 09:36:58	100
15	PRJ20201204000005	실용 - 고객사	김민준	Azure	2020/12/04 10:37:04	100
16	PRJ20201214000006	실용 - 고객사	김민준	Azure	2020/12/14 10:37:10	100
17	PRJ20201214000007	실용 - 고객사	김민준	Azure	2020/12/14 20:18:50	100
18	PRJ20201214000008	실용 - 고객사	김민준	Azure	2020/12/14 08:55:44	100
19	PRJ20201209000009	실용 - 고객사	김민준	Azure	2020/12/09 16:28:13	100
20	PRJ20201208000010	실용 - 고객사	김민준	Azure	2020/12/08 10:32:59	100

[Azure에서 자주 발생하는 취약한 설정들]

- 모든 퍼블릭 액세스 차단
 - 이 설정을 활성화하면 아래 4개의 설정을 모두 활성화한 것과 같습니다. 다음 설정 각각은 서로 독립적입니다.
 - 생ACL(엑세스 제어 목록)을 통해 부여된 바깥 및 객체에 대한 퍼블릭 액세스 차단
 - 53은 새로 추가된 것으로 -1에 의해 적용되는 퍼블릭 액세스 공인물 사용이며, 기존 바깥 및 객체에 대한 퍼블릭 액세스 ACL 설정을 유지합니다. 이 설정을 ACL을 사용하여 53 리소스에 대한 퍼블릭 액세스를 허용하는 것은 점검을 면하지 않습니다.
 - 읽기/쓰기(엑세스 제어 목록)을 통해 부여된 바깥 및 객체에 대한 퍼블릭 액세스 차단
 - 53은 바깥 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 ACL을 무시합니다.
 - 생 퍼블릭 바깥 또는 액세스 지정 정책을 통해 바깥 및 객체에 대한 퍼블릭 액세스 차단
 - 53은 바깥 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 정책을 무시합니다. 이 설정은 53 리소스에 대한 퍼블릭 액세스를 허용하는 것은 점검을 면하지 않습니다.
 - 읽기/쓰기 퍼블릭 바깥 또는 액세스 지정 정책
 - 53은 바깥 및 객체에 대한 퍼블릭 액세스를 부여하는 모든 액세스 지정에 대한 퍼블릭 및 교차 계정 액세스를 무시합니다.
- 모든 퍼블릭 액세스 차단을 비활성화하면 이 바깥과 그 안에 포함된 객체가 퍼블릭 상태가 될 수 있습니다. 정책 및 사이트 호스팅과 같은 구체적인 확인된 사용 사례에서 퍼블릭 액세스가 필요한 경우가 아니면 모든 퍼블릭 액세스 차단을 활성화하는 것이 좋습니다.
 - 현재 설정으로 인해 이 바깥과 그 안에 포함된 객체가 퍼블릭 상태가 될 수 있을 줄 알고 있습니다.

Azure Storage를 Public Access로 설정하는 경우

서버 이미지에 Public 접근 권한을 부여하는 경우

이미지 권한 수정

현재 이 이미지는 다음과 같습니다. 퍼블릭 프라이빗

방화벽 In-bound Rule을 Anywhere로 선택하는 경우

인바운드 규칙 1

유형 정보: 모든 트래픽 | 프로토콜 정보: 전체 | 포트 범위 정보: 전체

소스 유형 정보: 위치 무관 | 소스: 0.0.0.0/0 | 설정 - 선택 사항 정보: //0

고객사의 정보자산 보호를 위해 보안관제센터에서 실시간으로 위협을 탐지 및 대응하고, 클라우드 보안 기술 전문 인력이 보안관리 업무 서비스를 제공합니다.

컨설팅

구축

솔루션

운영관제

Q. 보안 사고는 어떻게 예방하나요?

A 정기적인 보안 점검 및 교육 홍보

- 취약성 점검 수행 및 개선 방안 제시
- 임직원의 정보보안 인식 제고를 위해 보안 정보 전파

Q. 위협을 실시간으로 탐지할 수 있나요?

A 24 x 365 실시간 보안 사고 모니터링

- 해킹/바이러스 실시간 탐지
- 위협 및 이상징후 모니터링을 위한 클라우드 Native 솔루션 활용 (Azure Defender 등)

Q. 재발 방지 도와주세요!

A 사고 원인 및 경로 분석을 통한 재발 방지

- 사고 원인 분석 및 보고, 전파
- 바이러스 확산 차단

Q. 사고 발생 시 대응에 어떤 도움을 받을 수 있나요?

A 즉각적인 보안 사고 대응 체계 마련 및 실행

- 사고 대응 체계에 따른 초기 사고 대응 진행
- 사고 분석을 통해 사고 확산 방지 및 피해 범위 최소화
- 사고로 인한 피해 복구 지원

2. 서비스 오퍼링 | Managed Service

해킹/악성코드 등 외부 위협을 실시간 감지 및 대응할 수 있는 관제 및 운영 서비스입니다.

