LG CNS

클라우드 보안

2021. 5.

LG CNS 보안기술전략팀 김연수 책임

Contents

클라우드 보안

디지털 전환의 일환으로 클라우드 전환이 가속화됨에 따라 클라우드 보안에 대한 우려가 커지고 있습니다.

클라우드 이용 확대에 따른
클라우드 보안에 대한 우려가 높습니다.

클라우드 환경에서의 보안

클라우드 서비스 제공자(CSP)와 클라우드 사용 기업 간의 역할과 책임이 구분되며, 이는 컴플라이언스에도 적용됨

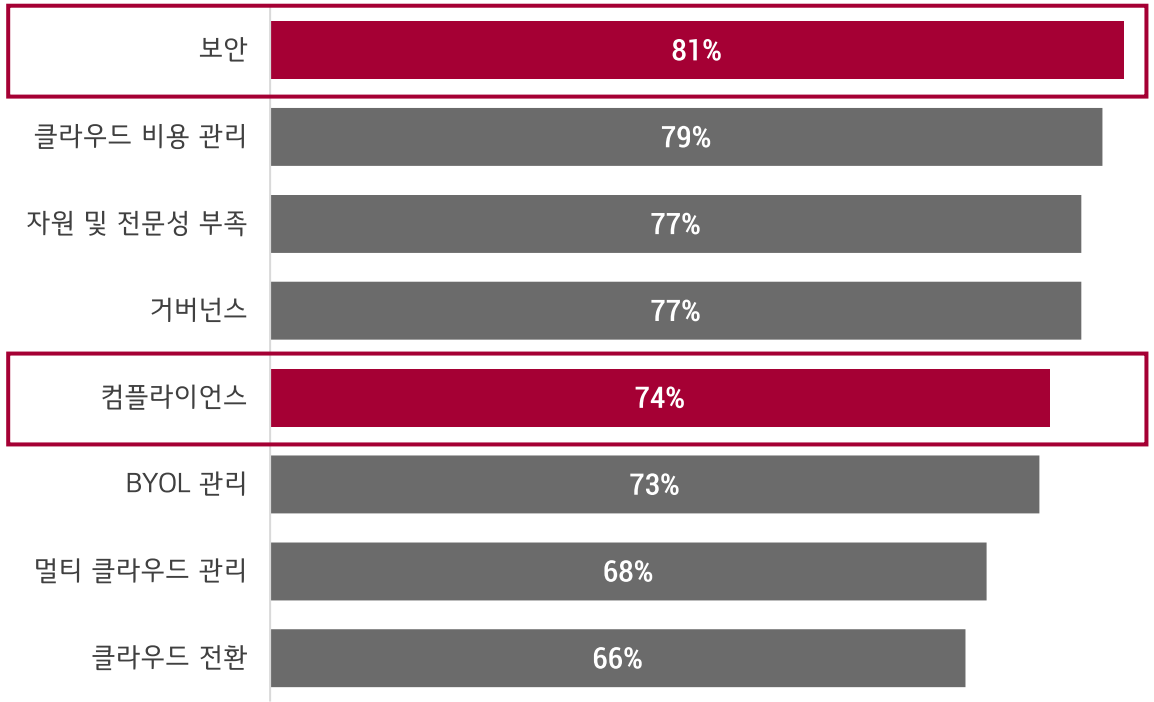
- CSP는 클라우드의 보안을 담당 (데이터센터의 물리적 보안 등)
- 클라우드 사용 기업은 클라우드에서의 보안을 담당 (가상환경 관리 등)

클라우드 사용 기업에서 클라우드 환경에 대한 전문성이 부족한 경우가 많음

- 클라우드 관리 미흡 및 설정 오류 등

기업의 클라우드 도입 및 활용 시 우려사항

[%, 중복응답가능]



Source: Flexera State of the Cloud Report (2020)

클라우드 보안 우려는 단순히 우려에 그치지 않고 실제 보안 사고로 이어지고 있습니다.

클라우드 보안 사고

> "2023년까지 최소 99%의 클라우드 보안 실패는 고객사 잘못에 의한 것"
>
> [가트너]

전자신문

2018년 07월 24일 화요일 010면 종합

클라우드 사용 기업 절반 '보안 먹구름'

김인순 insoon@
보안 전문기자

스토리지 설정 오류…데이터 유출 빈번
비번 설정 안 해 해커에게 문 열어준 꼴

美 테슬라·英 보험사 아비바 등
악성코드 감염 '암호화폐 채굴' 악용

올해 상반기에 클라우드 사용 기업 절반이 사이버 공격을 당한 것으로 나타났다. 기업이 데이터와 애플리케이션을 클라우드 인프라로 이동, 해커도 서버와 PC에 국한시킨 공격을 클라우드 인프라로 확대했다.

체크포인트는 2018년 상반기 사이버 공격 보고서를 통해 전 세계 기업·기관 51%가 클라우드 인프라 대상으로 사이버 공격을 당했다고 23일 밝혔다. 이에 따르면 해커는 클라우드 스토리지 서비스를 악용, 다양한 공격과 기술을 시도했다. 페덱스, 아비바, 혼다, 테슬라 등이 클라우드 인프라 공격을 받았다.

기업은 클라우드 인프라로 이동했지만 아직 최적화한 보안 체계를 갖추지 못했다. 클라우드 스토리지 설정 오류로 중요한 외부 데이터를 유출하는 사고가 빈번한 실정이다.

해커는 컴퓨팅 파워가 큰 클라우드 인프라 취약점을 찾아내는 데 심혈을 기울이고 있다. 공격자는 주요 자료를 빼돌리는 것은 물론 암호화폐를 채굴했다. 클라우드 인프라는 암호화폐 채굴에 PC나 서버보다 훨씬 효율 높은 환경이다. 상반기에 클라우드 구성 핵심 요소인 '도커'와 '쿠버네티스'를 표적한 채굴 악성코드가 발견됐다.

전기차 기업 테슬라와 영국 다국적 보험사 아비바, 젬알토 등은 상반기 클라우드 인프라가 암호화폐 채굴 악성코드에 감염된 것으로 알려졌다. 세 회사는 오픈소스 쿠버네티스 관리자 콘솔을 사용했다. 문제는 인터넷으로 접속할 수 있는 서비스임에도 비밀번호를 설정하지 않았다. 클라우드 설정 오류로 해커에게 인프라 문을 그대로 열어 준 셈이었다.

해커가 기업 쿠버네티스 관리자 콘솔에 접근하면 아마존웹서비스(AWS)나 마이크로소프트(MS) 애저 환경에 접속하는 권한도 얻는다. 해커는 클라우드 인프라에 접근해 암호화폐 채굴 악성코드를 설치하고 컴퓨팅 파워를 빼돌렸다.

사이버 공격자는 테슬라가 사용하고 있는 AWS 환경에서 접속 권한을 발견했다. 테슬라 자동차의 민감한 텔레메트리 데이터가 저장된 아마존 심플 스토리지 서비스(S3) 버킷에 접속할 수 있었다. 테슬라는 발견 즉시 조치하고 고객 프라이버시나 차량 안전, 보안이 훼손된 흔적은 없다고 밝혔다.

클라우드 서비스 설정 오류로 인한 정보 유출 사고도 줄을 이었다. AWS S3를 비롯해 애저, 구글 등에 적용된 스토리지 설정 오류 때문이다. 고객은 AWS S3에서 사용하는 공간을 '버킷'으로 지정한다. 문제는 버킷을 구성할 때 사용자 오류로 내부 데이터가 유출된다. 버킷 설정을 읽기(Read) 상태로 두면 자동으로 데이터가 외부에 노출된다. 일부 사용자는 버킷을 덮어쓰는(overwrite) 설정으로 방치해 데이터가 삭제되거나 악성코드에 감염되는 더 큰 피해를 본다.

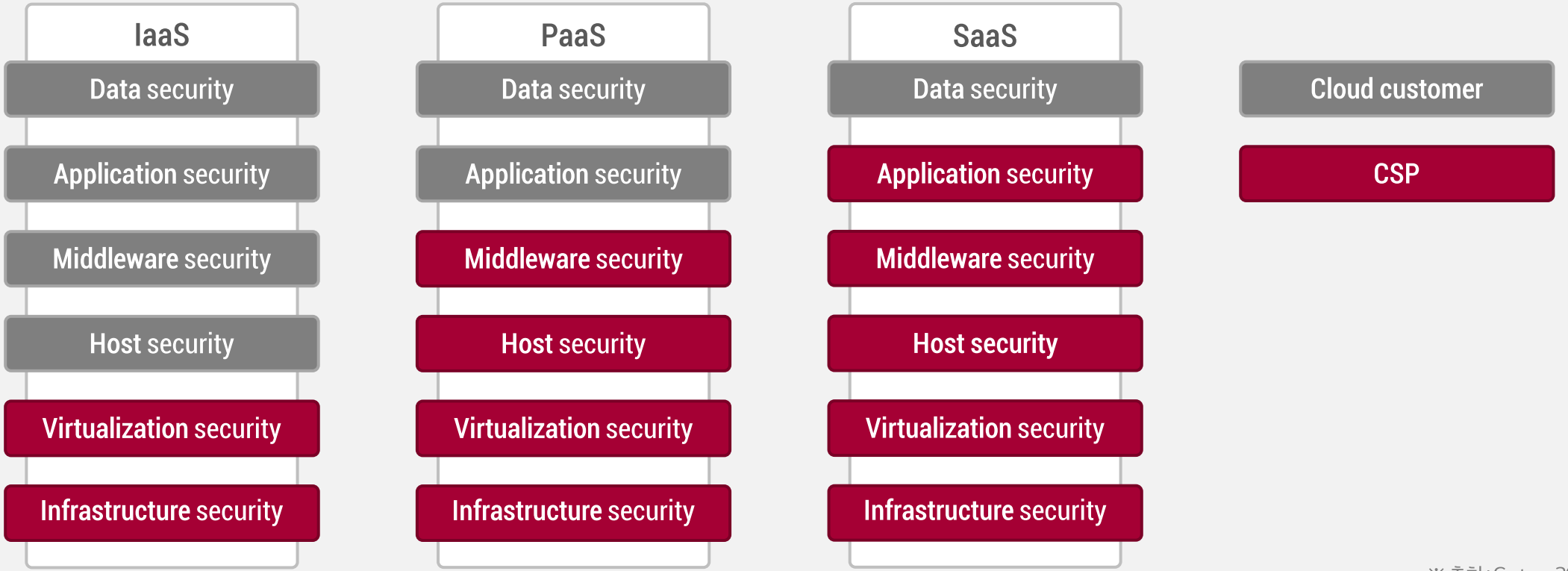
공격자가 수정 가능한 버킷을 찾아내면 악성코드를 업로드, 파일을 훼손시킨다. 해커는 잘못된 클라우드 스토리지 설정을 검색하는 도구 'AWS S3 버킷 덤프'도 사용한다.

지난해 1억9000만명의 미국 유권자 개인 정보를 인터넷에 노출한 사고 역시 클라우드 스토리지 설정 오류로 발생했다.

시점	내용	원인
'15년	넷플릭스 등 서비스 중단 (AWS 내부작업 중 장애)	CSP 실수
'16년	Azure 네트워크 SW 버그로 서비스 장애	CSP 실수
'17년	애플, 에어비앤비 서비스 중단 (AWS 관리자 실수)	CSP 실수
'18년	나이키, 쿠팡 서비스 중단 (AWS 서울리전 DNS 오류)	CSP 실수
'18년	혼다 자동차 개인정보 유출	클라우드 설정 오류
'18년	중국 텐센트 고객사 데이터 삭제	직원 실수
'19년	캐피탈원 개인정보 1억600만건 유출	클라우드 설정 오류
'19년	어도비 해킹으로 개인정보 약 300만명 유출	클라우드 설정 오류
'20년	App 개발사 실수로 Azure에 개인정보 노출	클라우드 설정 오류

클라우드 환경에서 보안은 클라우드 서비스 제공자(CSP)와 사용자가 보안 영역을 나누어 공동 책임지도록 되어 있으며, 사용자는 CSP의 보안 기능과 서비스를 이용하거나 3rd Party 보안 솔루션으로 보안을 스스로 챙겨야 합니다.

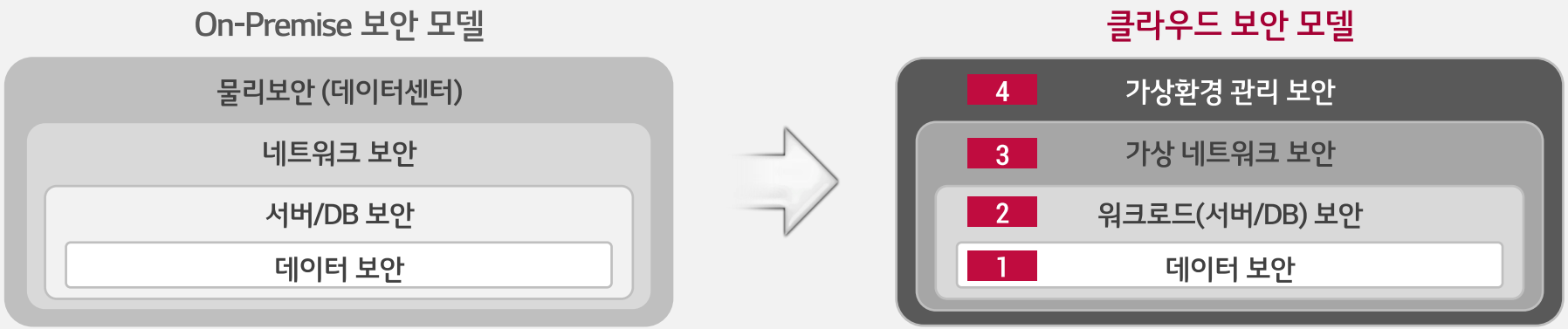
클라우드 보안 책임 공유 모델



※ 출처 : Gartner 2016

클라우드 보안은 물리보안 계층이 없는 대신 가상환경 관리 보안 영역이 새롭게 존재합니다.

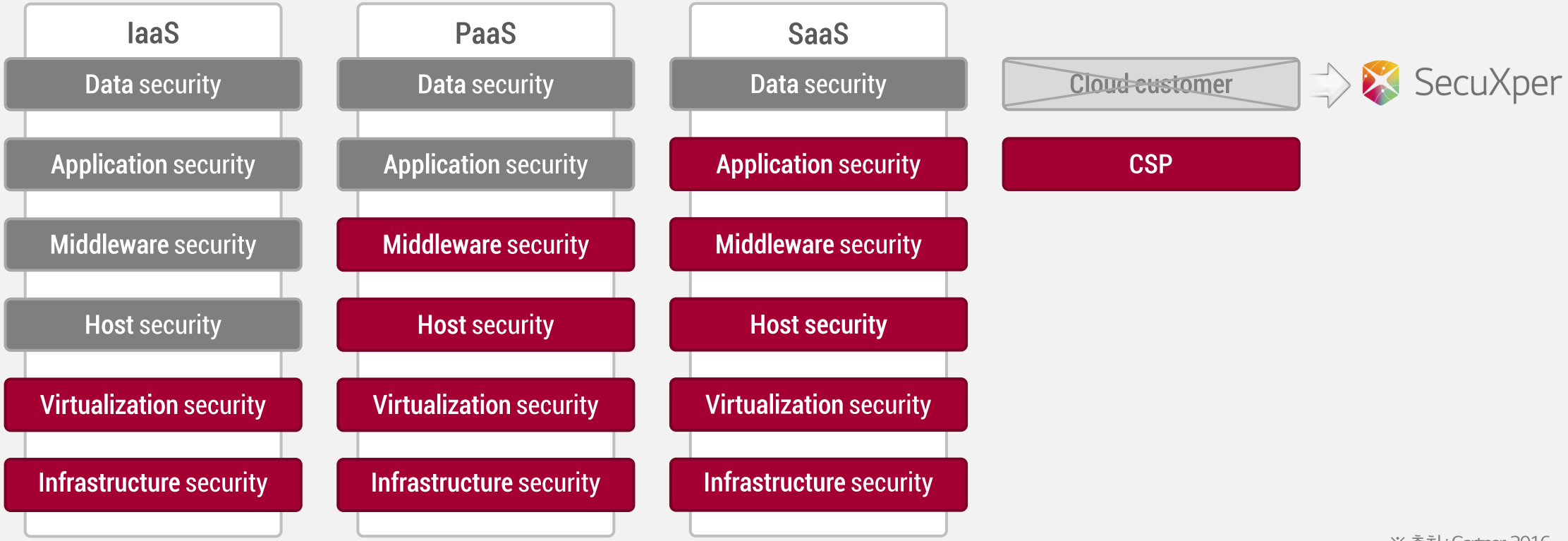
클라우드 보안의 특징



1	데이터 보안	기존 데이터 보안과 큰 차이는 없으나 암호화 대책 적용 방식에 차이가 있을 수 있음
2	워크로드 보안	서버 보안 뿐만 아니라 최근 많이 활용되는 컨테이너, 서버리스 보안 고려 필요
3	가상 네트워크 보안	SDN(Software Defined Network)으로 네트워크 설정 및 접근통제를 소프트웨어 방식으로 처리
4	가상환경 관리 보안	클라우드 자원 생성 시 각종 보안 설정에 대한 안전성을 점검하는 것이 중요

LG CNS의 클라우드 보안에 대한 접근은 클라우드 환경에서 고객이 책임져야 할 보안 영역을 LG CNS가 MSSP로서 고객을 대신하여 책임질 수 있는 서비스를 제공하는 것입니다.

LG CNS 클라우드 보안 방향



※ 출처 : Gartner 2016

2. 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

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

- AWS, Azure, GCP 클라우드 보안 설정 점검
- 국내 개인정보보호법 등 컴플라이언스 기준

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)

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.

컨설팅 | 구축 | 솔루션 | 운영관제

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

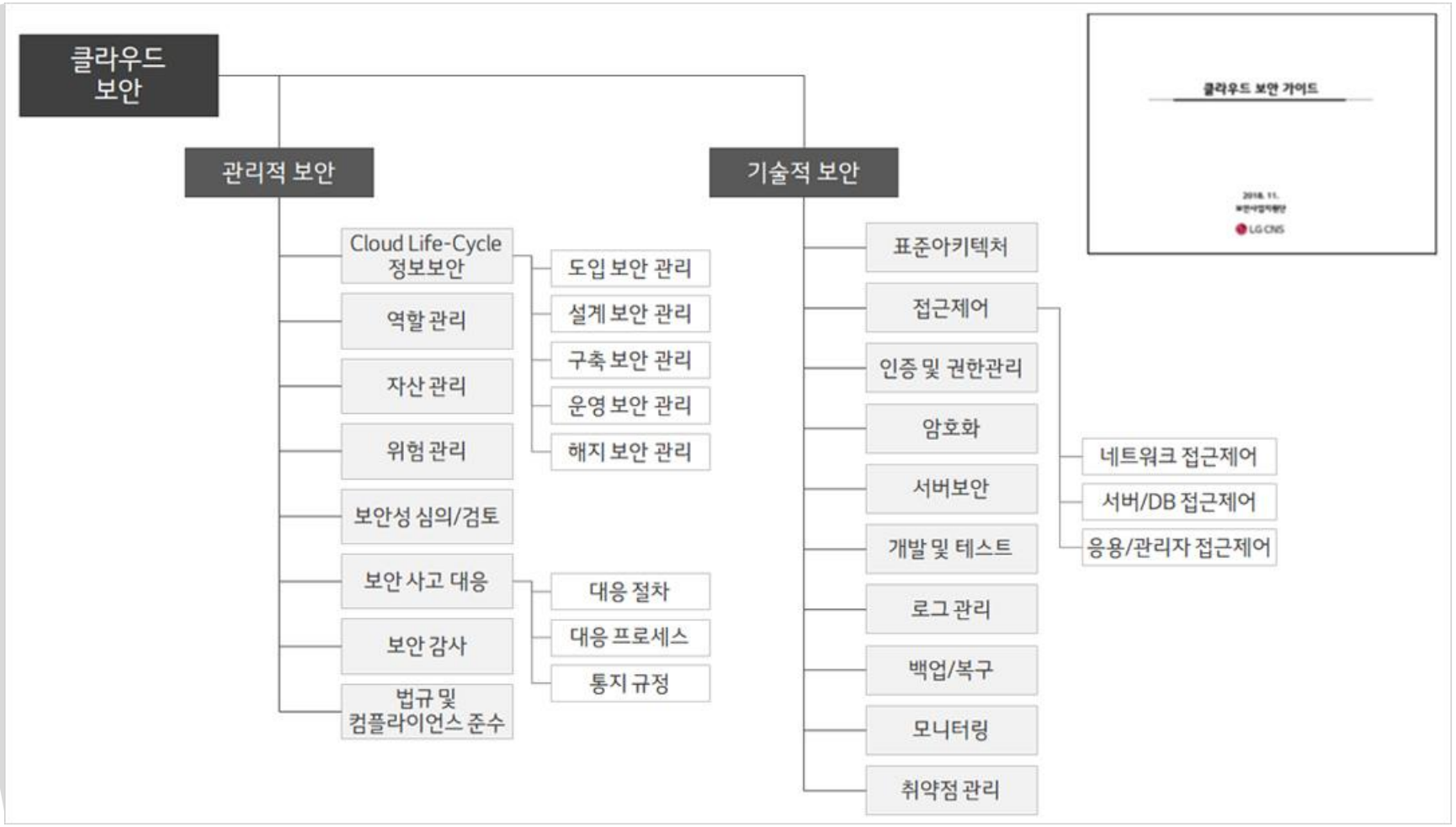
Certification Consulting

- 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.

컨설팅 | 구축 | 솔루션 | 운영관제

SecuXper
Cloud 컨설팅 서비스



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

컨설팅 구축 솔루션 운영관제

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 02 BCP 계획 수립 03 안정성 확보 조치 방안 수립 04 업무위탁 운영 기준 마련 05 서비스 제공자 평가 및 선정 06 정보위원회 심의/의결	11 위수탁 계약서 관련 주요 컴플라이언스 요건 확인 ▪ 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 ▪ 이용대상 및 중요도평가, 출구전략, 제공자 후보선정 및 평가 결과 등 14 서류 최신성 유지 및 수시 보고체계 수립 ▪ 관리 방안 및 보고 계획 등	20 Exit 이행 ▪ 수립 Exit 진단결과 및 이행 계획기준 Exit 이행
수행 결과	07 중요도 평가 기준 및 결과서 08 클라우드 이용 관련 BCP 계획 09 안정성 확보 조치 사항 결과 10 정보보호위원회 심의/의결	12 금융회사 업무위탁 관한 규정 제7조 제 1항 각호 관한 서류 ▪ 위탁계약서, 업무 위수탁 운영기준, 준법감시인 검토 의견 ▪ 위탁 필요성 및 기대효과 ▪ 위탁 따른 업무 절차 변경 내용	15 업무 위탁 규정 제7조 제1항 서류 16 중요도 평가 기준 및 결과서 17 클라우드 이용관련 BCP 계획서 18 안정성 확보 조치 사항 결과 19 정보보호위원회 심의/의결 결과	21 Migration ▪ 클라우드서비스 제공자 전환

2. 서비스 오퍼링 | Implementation

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

컨설팅 | **구축** | 솔루션 | 운영관제

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?

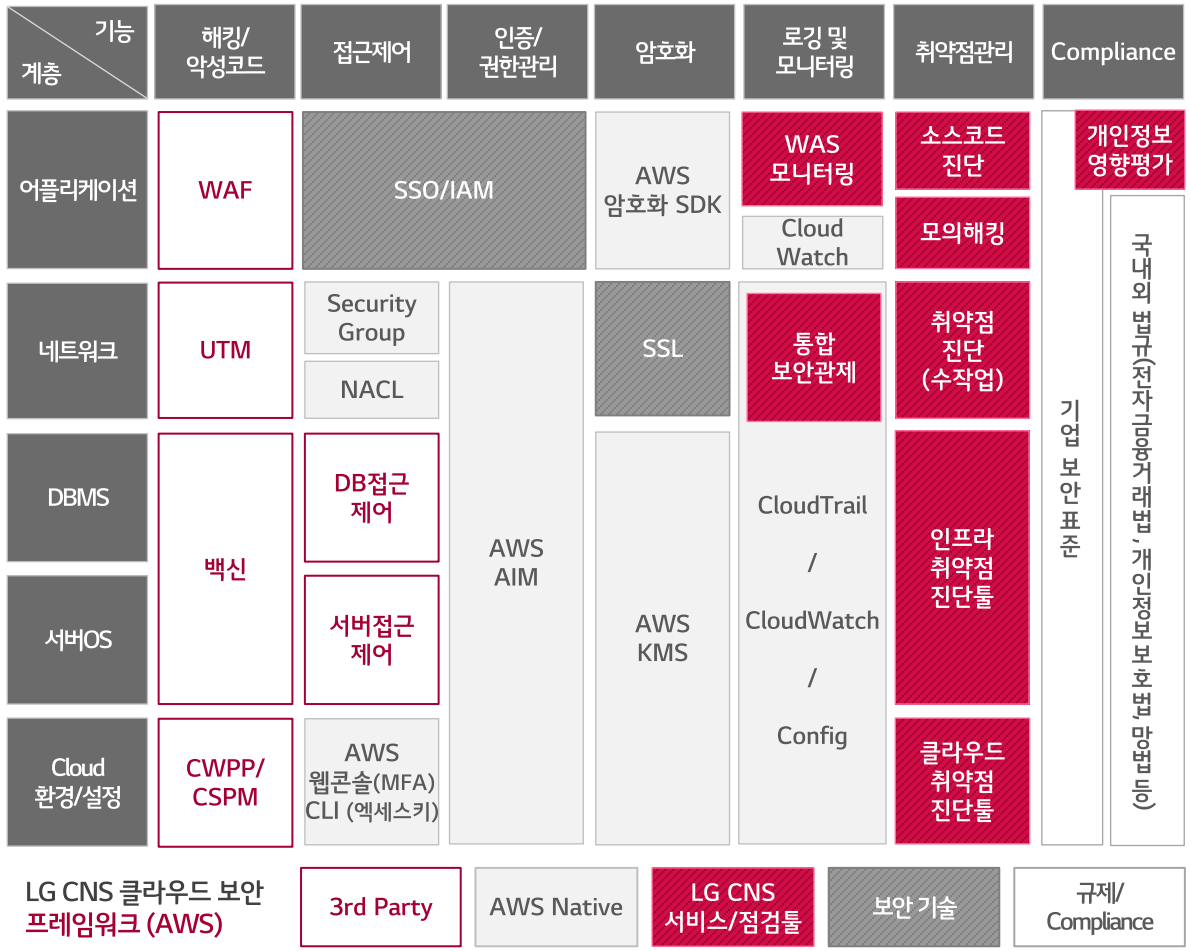
A Native 클라우드 보안 솔루션 선정

- 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?

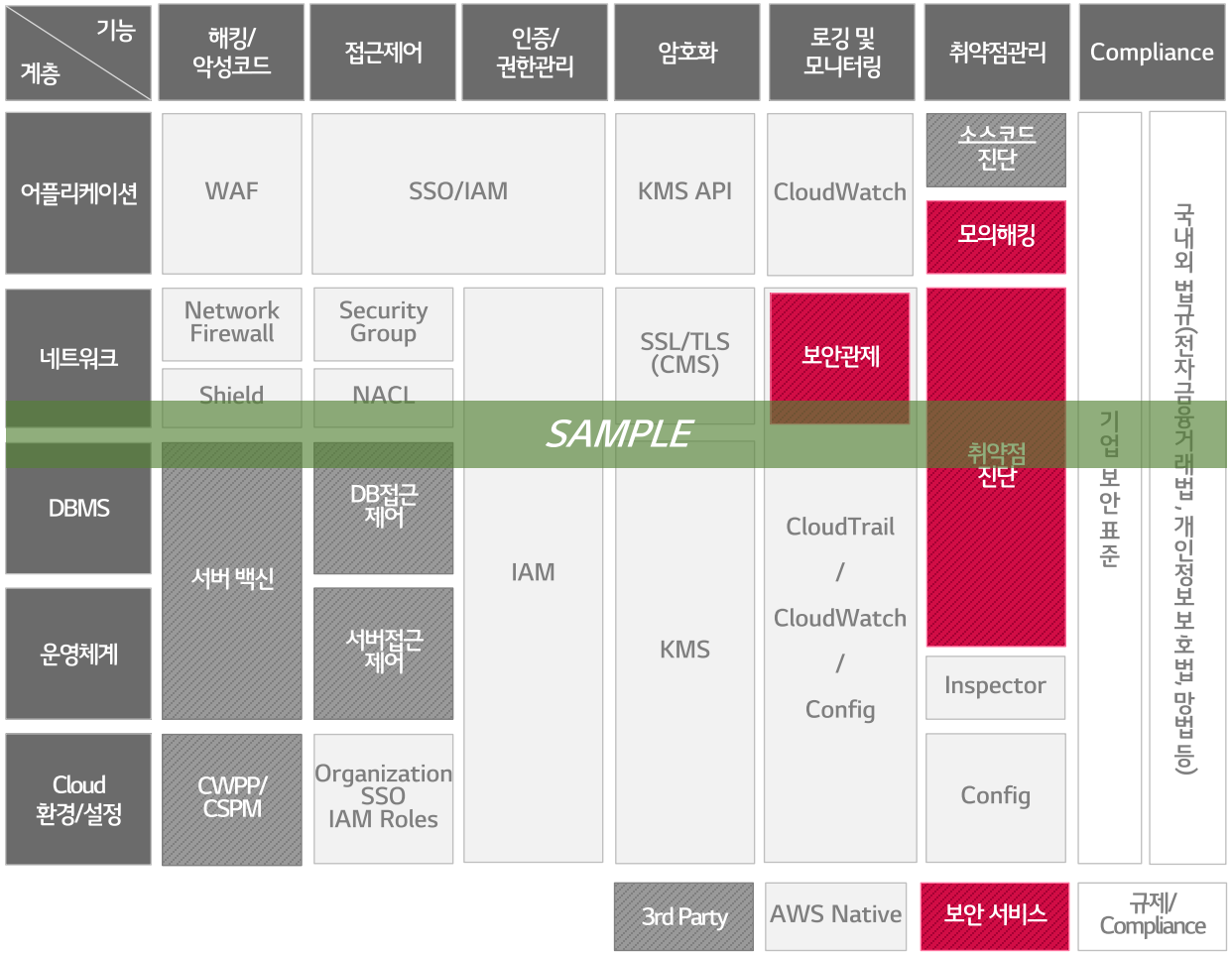
A Native 보안 기능 및 서비스 중점 구현

- 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



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

컨설팅 | 구축 | 솔루션 | 운영관제



Native 보안 서비스 우선 적용

- 최소한의 클라우드 보안통제를 위한 기본 Baseline 설정
  - 필수 보안기능 활성화 (예: CloudTrail)
- 글로벌 클라우드 서비스 제공자의 Threat Intelligence를 최대한 활용할 수 있는 Native 보안 서비스 적용 (예: GuardDuty)

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?

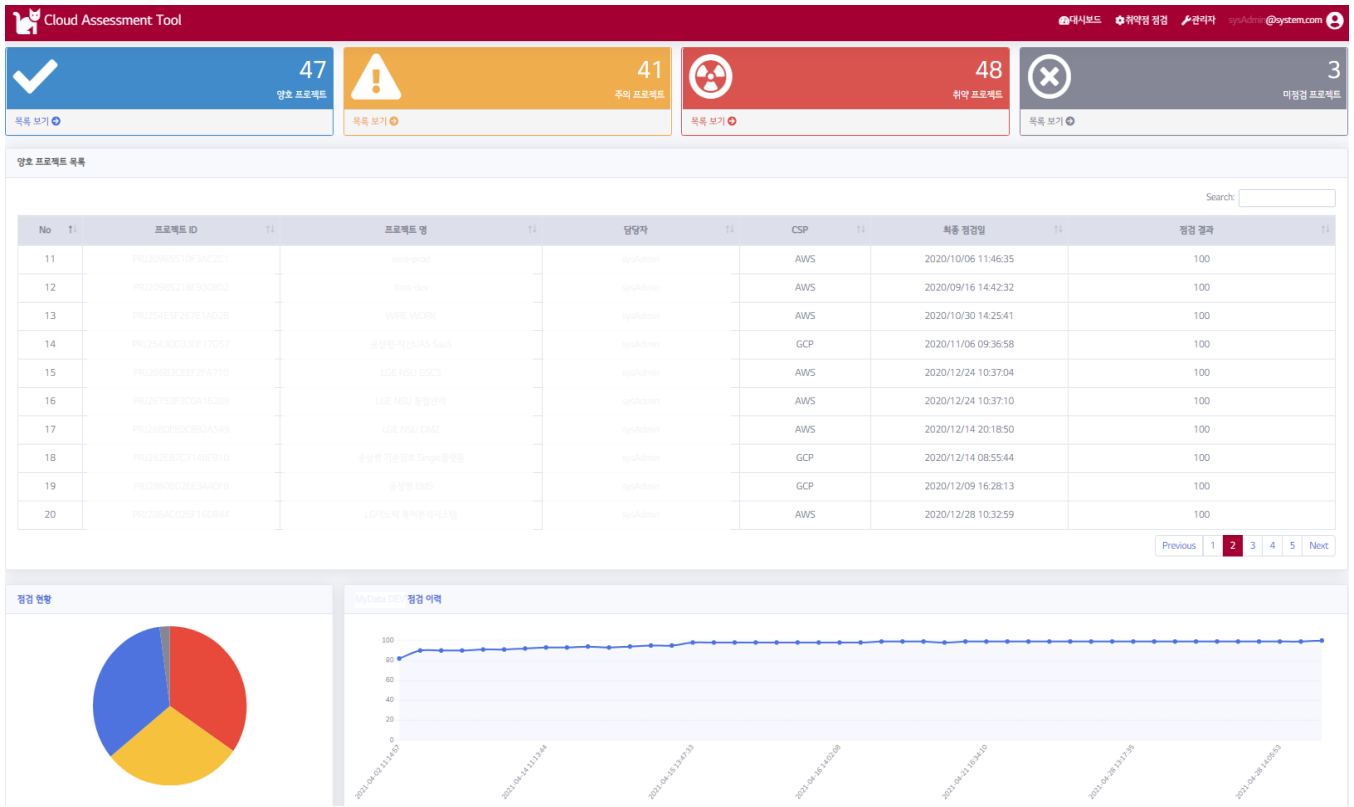
A

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

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

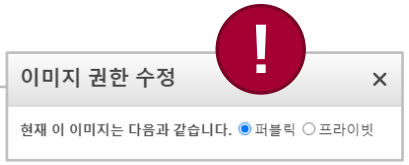
컨설팅 구축 **솔루션** 운영관제



AWS에서 자주 발생하는 취약한 설정들

S3 Bucket을
Public Access로 설정하는 경우

서버 이미지에
Public 접근 권한을 부여하는 경우



방화벽 In-bound Rule을
Anywhere로 선택하는 경우

2. 서비스 오퍼링 | Managed Service

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 (AWS GuardDuty 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

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

컨설팅 구축 **솔루션** 운영관제

보안관제센터

- 취약점 진단
- OS 패치 적용
- 보안 정보 전파

예방

탐지

- 24x365 보안사고 모니터링
- 해킹/바이러스 실시간 탐지

보안포털 보안분석시스템

- 원인분석 및 보고
- 사고전파
- 바이러스 확산 차단

재발 방지

대응

- 해킹사고 분석/복구 지원
- 신종 바이러스 조치

사고 예방

사고 탐지

고객

Network 보안

- 해킹 시도, DdoS 공격
- 웜바이러스 트래픽
- 비정상 트래픽

Endpoint 보안

- 예방: OS패치, 취약성 제거
- 웜바이러스 유입/유출 차단
- 통제 우회 및 비정상 행위

Web/Application 보안

- Web 해킹시도
- Web 서비스 정상 동작
- Web 위변조 여부

24 x 365 멈추지 않는 보안 운영/관제 서비스

검증된 보안 전문가 집단이 고객사에 최적화된 클라우드 보안 환경을 구현합니다.

클라우드 보안 전문성

기술 이해와 업무 노하우를 축적한 업계 최고 수준의 보안 전문 인력 다수 보유

- 컨설팅부터 운영관리까지, 클라우드 보안 全 프로세스에서 다양한 수행 경험을 보유한 LG CNS 보안 전문 인력이 직접 수행
- **RED팀 :** 침입 탐지 및 취약점 진단 서비스를 제공하는 전문가 그룹 (화이트 해커)

고객의 비즈니스 환경에 최적화된 클라우드 정보보안 모델 설계 및 구축/운영

- 클라우드 전문성을 기반으로 고객사 환경에 적합한 CSP 솔루션 및 서비스 선정 및 구현
  - 글로벌 CSP와의 파트너십 : AWS, MS Azure, Google Cloud, Oracle Cloud 등
  - AWS Security Competency Consulting 인증 ('20)

LG CNS의 화이트 해커, RED팀

- 국내외 화이트 해커 대회 참여 및 수상
  - 데프콘, 코드게이트, HDCON 등
- 취약점 자동 진단 도구 개발
  - KISA 신규 점검항목 진단
- KISA 개발보안 자문위원 활동 중

글로벌 CSP와의 파트너십

aws
Microsoft Azure
Google Cloud
ORACLE CLOUD

퍼블릭 클라우드 보안 전문성 인증

aws partner network
Consulting Partner
Security Competency

Digital Innovation Enabler

Thank You

LG CNS