

PISAP - ECSA Training

ECSA Advanced Course (Module 1, 2)

박병화 (bhpark@amazon.com)

Sr. Security Consultant

AWS Professional Services Korea

Training Course

PISAP

Proserve Infrastructure & Security Advanced Partner

01



02



03



04



05



06



PISAP

Proserve Infrastructure & Security Advanced Partner

01

02

03

04

05

06

ECSA

Enhanced Cloud Security
Assessment

AWS Cloud Infra & Service &
Application 영역에서의 보안
진단

Prowler 를 이용한 BP 기준
진단



AWS 보안의 첫 시작

PISAP

Proserve Infrastructure & Security Advanced Partner

01

ECSA

Enhanced Cloud Security
Assessment

AWS Cloud Infra & Service &
Application 영역에서의 보안
진단

Prowler 를 이용한 BP 기준
진단



02

ECIA

Enhanced Cloud Infrastructure
Assessment

AWS Cloud Infra 의 네트워크
진단 과 보안 고도화 향상

AWS BP 를 적용하고 고객의
요구사항을 기반한 보안 진단



03



04



05



06



AWS 인프라의 보안
고도화

PISAP

Proserve Infrastructure & Security Advanced Partner

01

ECSA

Enhanced Cloud Security
Assessment

AWS Cloud Infra & Service &
Application 영역에서의 보안
진단

Prowler 를 이용한 BP 기준
진단



02

ECIA

Enhanced Cloud Infrastructure
Assessment

AWS Cloud Infra 의 네트워크
진단 과 보안 고도화 향상

AWS BP 를 적용하고 고객의
요구사항을 기반한 보안 진단



03

ECDSA

Enhanced Cloud Database & Security
Assessment

AWS Cloud DB 환경에 대한
진단과 보안 고도화 향상



04



05



06



AWS Database
보안 진단

PISAP

Proserve Infrastructure & Security Advanced Partner

01

ECSA

Enhanced Cloud Security Assessment

AWS Cloud Infra & Service & Application 영역에서의 보안 진단

Prowler 를 이용한 BP 기준 진단



02

ECIA

Enhanced Cloud Infrastructure Assessment

AWS Cloud Infra 의 네트워크 진단 과 보안 고도화 향상

AWS BP 를 적용하고 고객의 요구사항을 기반한 보안 진단



03

ECDSA

Enhanced Cloud Database & Security Assessment

AWS Cloud DB 환경에 대한 진단과 보안 고도화 향상



04

ECIRA

Enhanced Cloud Incident Response Assessment

AWS Cloud Infra & Service & Application 환경의 사고 식별, 대응, 분석 자동화 및 보안 대시보드 구성

보안관제 고도화를 통한 위협 식별과 대응을 통하여 사고에 대한 높은 가시성을 제공



05



06



AWS 환경에 대한
사고대응 고도화

PISAP

Proserve Infrastructure & Security Advanced Partner

01

ECSA

Enhanced Cloud Security Assessment

AWS Cloud Infra & Service & Application 영역에서의 보안 진단

Prowler 를 이용한 BP 기준 진단



02

ECIA

Enhanced Cloud Infrastructure Assessment

AWS Cloud Infra 의 네트워크 진단 과 보안 고도화 향상

AWS BP 를 적용하고 고객의 요구사항을 기반한 보안 진단



03

ECDSA

Enhanced Cloud Database & Security Assessment

AWS Cloud DB 환경에 대한 진단과 보안 고도화 향상



04

ECIRA

Enhanced Cloud Incident Response Assessment

AWS Cloud Infra & Service & Application 환경의 사고 식별, 대응, 분석 자동화 및 보안 대시보드 구성

보안관제 고도화를 통한 위협 식별과 대응을 통하여 사고에 대한 높은 가시성을 제공



05

ECCSA

Enhanced Cloud Container & Security Assessment

AWS Container 환경에 대한 Proserve BP 를 통한 보안 수준 진단

Container 환경의 보안을 고도화



06



AWS 컨테이너 환경
보안 고도화

PISAP

Proserve Infrastructure & Security Advanced Partner

01

ECSA

Enhanced Cloud Security Assessment

AWS Cloud Infra & Service & Application 영역에서의 보안 진단

Prowler 를 이용한 BP 기준 진단



02

ECIA

Enhanced Cloud Infrastructure Assessment

AWS Cloud Infra 의 네트워크 진단 과 보안 고도화 향상

AWS BP 를 적용하고 고객의 요구사항을 기반한 보안 진단



03

ECDSA

Enhanced Cloud Database & Security Assessment

AWS Cloud DB 환경에 대한 진단과 보안 고도화 향상



04

ECIRA

Enhanced Cloud Incident Response Assessment

AWS Cloud Infra & Service & Application 환경의 사고 식별, 대응, 분석 자동화 및 보안 대시보드 구성

보안관제 고도화를 통한 위협 식별과 대응을 통하여 사고에 대한 높은 가시성을 제공



05

ECCSA

Enhanced Cloud Container & Security Assessment

AWS Container 환경에 대한 Proserve BP 를 통한 보안 수준 진단

Container 환경의 보안을 고도화



06

ECASA

Enhanced Cloud Gen-AI Security Assessment

AWS Cloud 운영환경에 대한 Gen-AI 을 이용한 보안 수준 진단 및 보안성 향상 가속화



Gen-AI 기반 보안성
가속화

ECSA Advanced Training Overview

- 교육 개요 (Module 1 + Module 2)
 - Control Tower 기반의 Landing Zone 구축 및 AWS Native 보안서비스 심화 교육
- 교육 기간 : 2025.1.13 ~ 2025.1.24 (10일)
- AWS 강사진 : 총 6명
 - 박병화, 김수종, 김웅식 (Security Consultant)
 - 허진성, 임규철, 신안셀모 (Cloud Architect)
- 교육 대상 : 총 18명
 - CloudNetworks 5명, KTDS 2명, 퍼시몬랩 3명
 - LG CNS 1명, 디딤기술 1명, 에스넷 1명, GSITM 1명
 - 이테크시스템 3명, 에티버스러닝 1명



Training Objectives

AWS Multi-Account 전략에 따른 보안 거버넌스를 이해하고, 대규모 클라우드 마이그레이션의 기본이 되는 랜딩존 구축 프로젝트를 직접 수행할 수 있는 능력 확보

AWS 계정 구조	표준화된 AWS 계정구조에 따른 통합적인 AWS 계정관리 및 신규 계정 발급 자동화 체계
지속 가능한 보안 및 거버넌스 구성	고객사 보안 표준에 맞는 전사 가드레일 및 거버넌스 정책을 중앙집중식으로 관리하도록 구현
통합 네트워크 구성	중앙 집중식 및 분산형 네트워크 아키텍처 설계 및 구현
보안 서비스	각종 AWS 보안 서비스의 소개 및 실습을 통한 체계적인 클라우드 보안 체계 구현
중앙 집중 로그 관리	AWS 인프라 및 어플리케이션용 로그의 중앙 집중식 저장 및 관리 체계 소개

Backlogs

- 흔히 해야할 일의 목록 또는 미처 처리 못한 일들이라고 생각
- 개발할 기능 또는 프로젝트/제품에서 요구하는 기능과 우선순위
- List of Outcomes, group by major outcomes, with criteria of acceptance

Area	4월			5월				6월				7월		
	W3	W4	W5	W1	W2	W3	W4	W1	W2	W3	W4	W5	W1	W2
	Planning	Sprint1		Sprint2		Sprint3		Sprint4		Sprint5		Sprint6		Closing
	4/12-4/14	4/18~4/29		5/2~5/13		5/16~5/27		5/30~6/10		6/13~6/24		6/27~7/8		7/11~7/14
Common	프로젝트 계획수립	AWS 현황 및 요건분석		Control Tower 가이드		Control Tower 구성		CfCT 구성		가드레일 최적화		Control Tower 최적화 (Automation)		종료보고 메가존 인수인계
		Account/OU 설계		CfCT 가이드		가드레일 테스트		가드레일 적용		모니터링 아키텍처		System Operation 가이드		
		Tagging 설계		가드레일 설계		Account 등록		Tagging/Backup 정책						
Platform		네트워크 아키텍처 기본설계		VPC/Subnet/CIDR 설계		네트워크 설계 보완		랜딩존 네트워크 구성 (계속)		AWS 감사로깅 아키텍처		AWS 감사로깅 아키텍처 (Update)		
				Connectivity 설계		Direct Connect 구성								
				DNS/Route 53 가이드		랜딩존 네트워크 구성								
Security		보안 요구사항 확인		SSO Permission Set 설계		Common Security Group 가이드		Common Security Group 적용		AWS 보안서비스 구성		침해사고대응 체계		Billing 권한분리/ Permission Set 반영 AWS 보안서비스 구성
		Shield/WAF/NFW 가이드		Encryption		SSO/AD 연계테스트		SSO/AD 구성		Billing 권한분리/ Permission Set 반영				
				Security Enabement (ANFW/WAF/GuardDuty)		Security Enabement (ANFW/WAF)		Firewall Manager Inspector 가이드 Security Hub, Detective 가이드						

Epic		Story
Sprint 1		
W1	Common	랜딩존 워크샵, Account 구조 및 OU 구조 가이드
	Common	고객사 인프라, 네트워크, 자동화 현황 분석 및 요구사항 확인
	Security	보안 워크샵
	Security	고객사 보안 요구사항 확인
W2	Security	고객사 보안 규정 및 가이드라인 분석
	Security	Network Firewall 가이드
	Platform	네트워크 아키텍처 가이드 - VPC(Draft), CIDR
	Platform	네트워크 아키텍처 설계 - VPC(Draft), CIDR
	Common	Naming Convention, Tagging Convention 가이드
Sprint 2		
W3	Security	Identity and Access Management 워크샵
	Security	암호화 적용 범위 및 키 관리 방안
	Platform	네트워크 아키텍처 가이드 - VPC, Egress/Ingress, DX/VPN
	Common	Region, AZ 정의
	Common	OU 구조 정의
	Common	Account 구조 정의
W4	Common	Naming Convention, Tagging Convention 정의
	Platform	네트워크 라우팅 가이드 (Subnet, TGW)
	Platform	네트워크 아키텍처 설계 - VPC (Sharing, Endpoint)
	Platform	인프라 구성 자동화 가이드 - VPC, EC2
	Security	보안 Baseline 검토
	Security	AWS Security Service 검토 Workshop
Sprint 3		
W5	Common	컨트롤 타워 구성 (Dev)
	Common	컨트롤 타워 파이프라인 구성 (CFCT)

Training Curriculum

	일차	시간	강의실	9:30 - 11:30 (2h)	1:00 - 3:00 (2h)	3:30 - 5:30 (2h)
1주차	Day 1	1/13(월)	에티버스 교육장 (학동)	Opening, Interview, Backlogs 소개	VPC Overview, EndPoint	Workshop AWS General/Network Immersion Day
	Day 2	1/14(화)	에티버스 교육장 (학동)	IAM Overview	IAM Workshop	EKS Fundamental
	Day 3	1/15(수)	에티버스 교육장 (학동)	Security Service Overview	KMS/ACM	GuardDuty & Hands-on
	Day 4	1/16(목)	에티버스 교육장 (학동)	Shield & WAF	WAF Hands-on	Logging & Monitoring (CloudTrail, CloudWatch, Athena, Security Hub, OpenSearch)
	Day 5	1/17(금)	에티버스 교육장 (학동)	Route53	Multi VPC Architecture	Multi VPC Connectivity
2주차	Day 6	1/20(월)	에티버스 교육장 (학동)	GWLB	Network Firewall	Network Firewall
	Day 7	1/21(화)	에티버스 교육장 (학동)	Multi-account strategy / Organizations	Control Tower Hands-on	Control Tower Hands-on
	Day 8	1/22(수)	에티버스 교육장 (학동)	Check Ride 과제 수행		
	Day 9	1/23(목)	에티버스 교육장 (학동)	Check Ride 과제 수행		
	Day 10	1/24(금)	에티버스 교육장 (학동)	Check Ride 발표 & 이론 시험 & 리소스 정리		

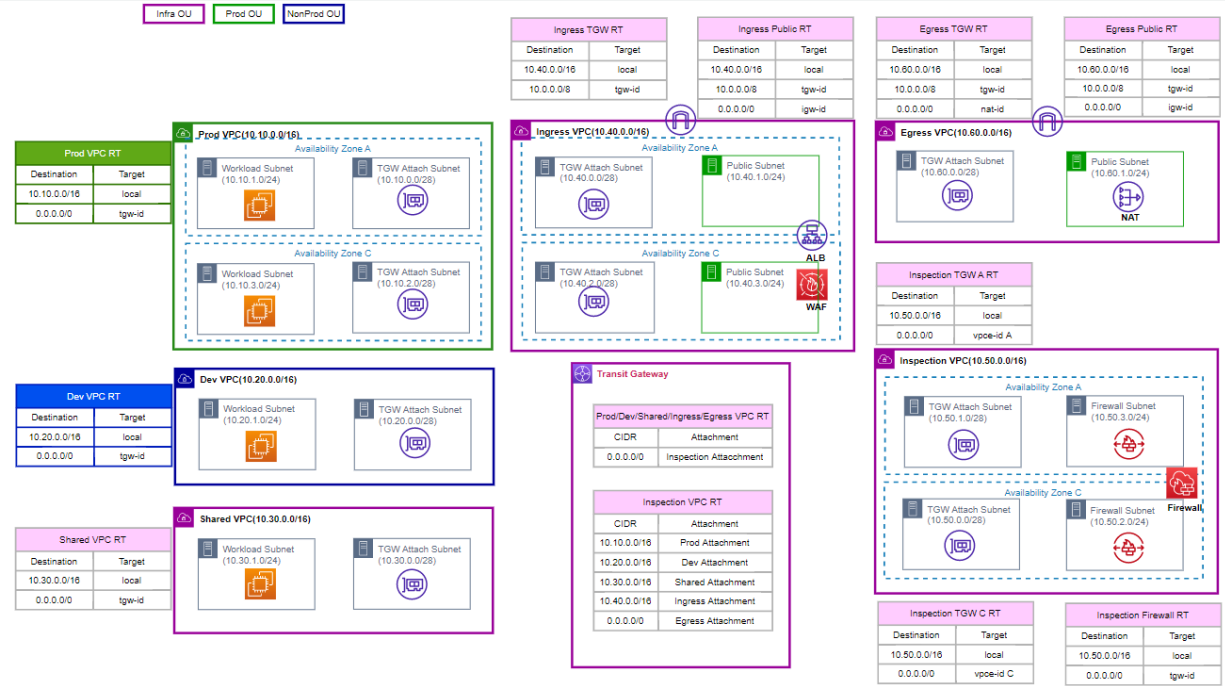
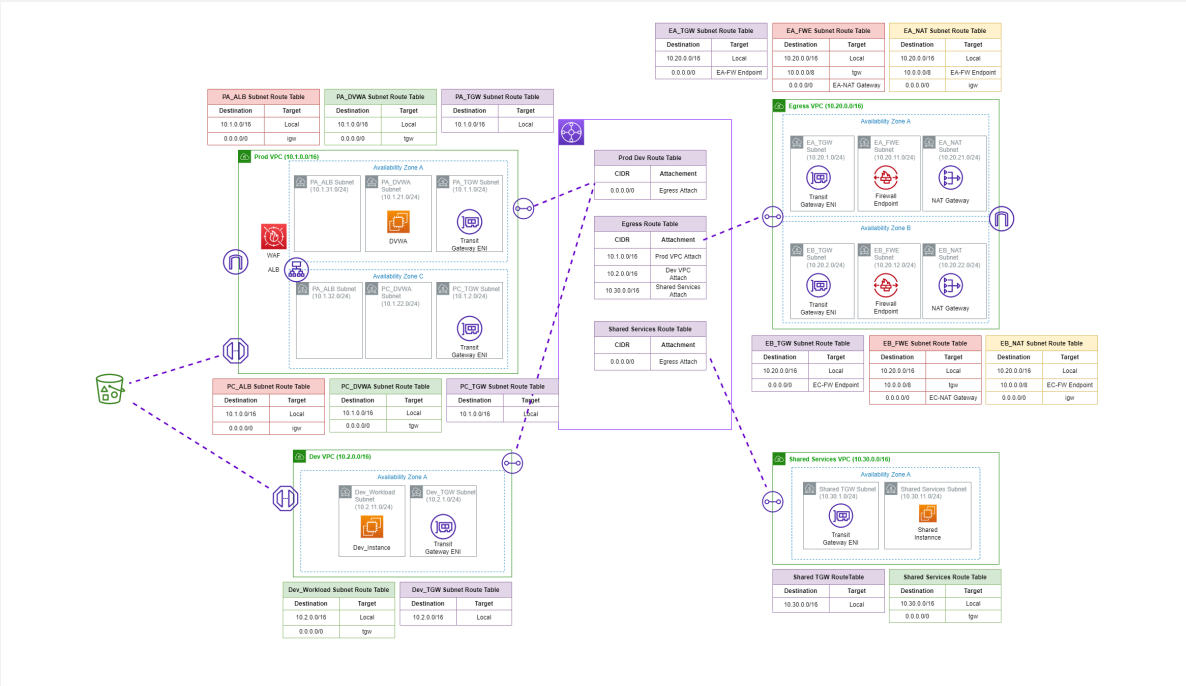
Check Ride 목적

- Check Ride는 본 교육 과정을 종합적으로 복습할 수 있도록 흥미와 의지를 유도함
- 종합적으로 랜딩존의 큰 그림과 여기에 올라가는 AWS Native Security 를 이해시키는 목적
- [이론] 이해한 내용에 대해 Cahoot을 이용한 이론 시험 수행 (객관식, 타임어택)
- [실기] 멤버들 간 서로의 아키텍처를 리뷰 및 토의하면서 이해도 향상
- 수업시간에 미처 설명하지 못한 유익한 정보 추가 제공 (Tip)
- 학습교육 전반에 대한 회고 및 자유로운 Discussion

Check Ride 구성 내용

구분	내용
Multi-Account 구조	Control Tower OU Best Practice에 따른 설계
회사 클라우드 보안 규정 준수	고객사 클라우드 보안 규정에 따른 가드레일 설계 및 구현
IAM Identity Center(Single Sign-On)	AWS SSO 설계 및 구현
통합 네트워크 아키텍처	Ingress 및 Egress 네트워크 통합 아키텍처 설계 및 구현
보안서비스 구축	AWS Native 보안 서비스에 대한 설계 및 구현 <ul style="list-style-type: none"> - GuardDuty - Network Firewall - WAF - Firewall Manager - Inspector - Security Hub
로깅 전략	보안 로그에 대한 Centralized Logging 구현

Check Ride 수행결과 - Network Architecture 부분



Professional Services Training의 특징

- 교육생 특기와 상관없이 개인별로 Check Ride의 모든 과제 영역을 수행
- 실제 프로젝트 수행과정에서 일어나는 상황들에 대한 Use case를 기반으로 설명
- 교육용 Workshop Studio를 적극 활용 (비용발생x)
- Workshop Studio로 불가능한 Control Tower기반의 실습은 실제 개인 계정(Gmail 권고)에서 수행
- Check Ride의 내용은 실제 프로젝트에서 수행한 내용을 축소하여 Mini Project 형식으로 구성
- Check Ride 시 발생하는 비용에 대해서 회사 내부적으로 처리할 수 있도록 사전 협의 요청

Ice Breaking



특공유격 2일 차

유격 끝판왕! 화생방 훈련

1. 자기 소개 (회사, 성함, 직무)
2. AWS 경험 (N/A, Test, Pjt)
3. 보안 솔루션 경험 (FW, WAF, IDS, IPS, DDoS 등)
4. 기타 (교육에 바라는 점)

여긴 어디... 나는 누구...?

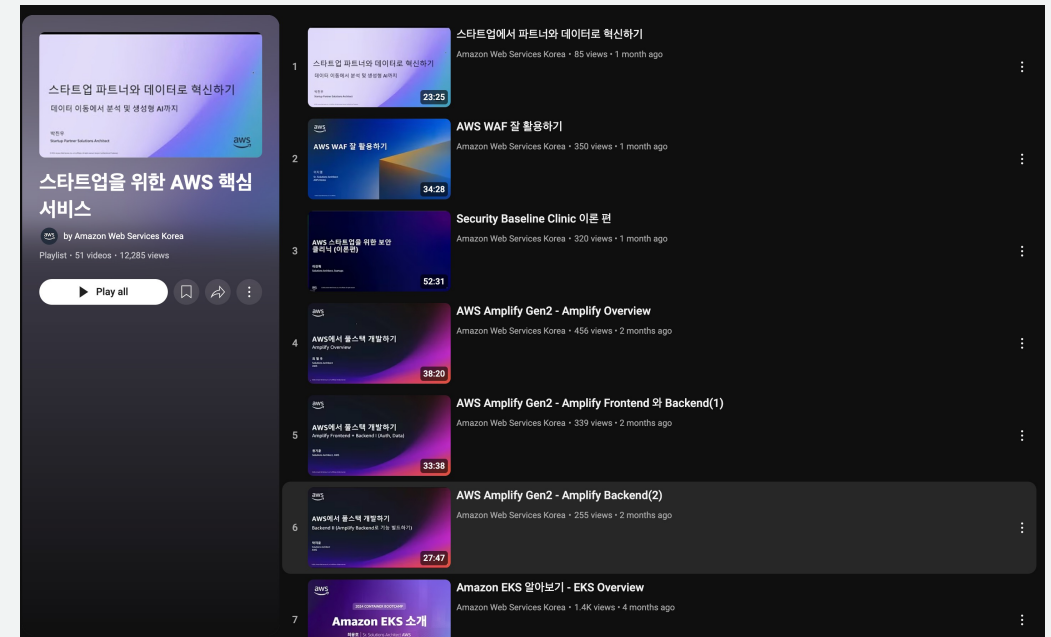
4.주요 공지 사항

- 1.본 과정 중 **Control Tower 환경 및 기타 구성 과제 구현(Checkride)**은 **개인 AWS 계정으로만 진행이 가능합니다.** 그러므로, 교육 사전에 수강생은 가급적 gmail을 이용하여 개인 AWS 계정을 발급하여 참석 부탁 드리겠습니다.
- 2.실습 진행 중 **구현 아키텍처에 따라 소정의 AWS 사용료(10만원 내외)가 과금될 수 있으므로, 이에 대한 내부 처리 방안을 확인 후 참석 바랍니다.**
- 3.본 과정은 실제 AWS 프로젝트 수행을 진행하기 위한 실무 과정입니다. 그러므로, AWS와 클라우드 환경에 익숙한 수강생의 참여를 권장 드리며, 강의 참여 전 하기 강의를 필수적으로 숙지 후 참석 부탁 드립니다.

https://www.youtube.com/playlist?list=PLORxAVAC5fUWoPJqJxJavUNK_QI8EFWP

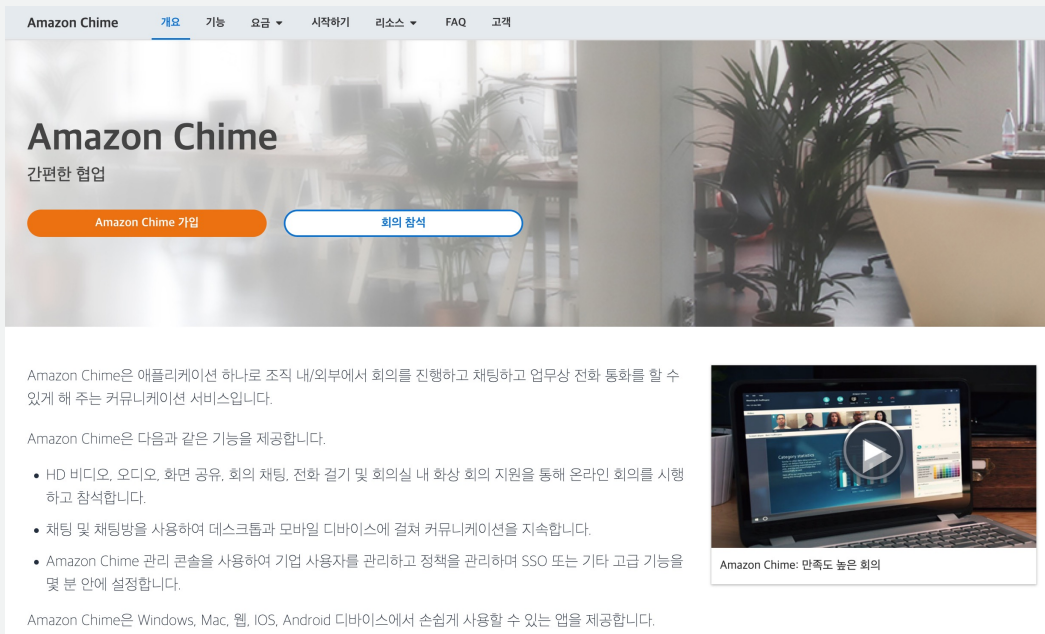
- Amazon EC2부터 서버리스 컴퓨팅까지, AWS 컴퓨팅 서비스 알아보기
- AWS의 스토리지, 데이터베이스 개념 잡기
- AWS를 사용한다면 반드시 알아야 할 네트워크 기초 지식
- 여러분이 가장 주목해야 하는 Security, 보안 개념 잡기

https://www.youtube.com/playlist?list=PLORxAVAC5fUWoPJqJxJavUNK_QI8EFWP



Communication Way

- Amazon Chime - 파일공유, 화상/텍스트 채팅



Amazon Chime

간편한 협업

Amazon Chime 가입 회의 참석

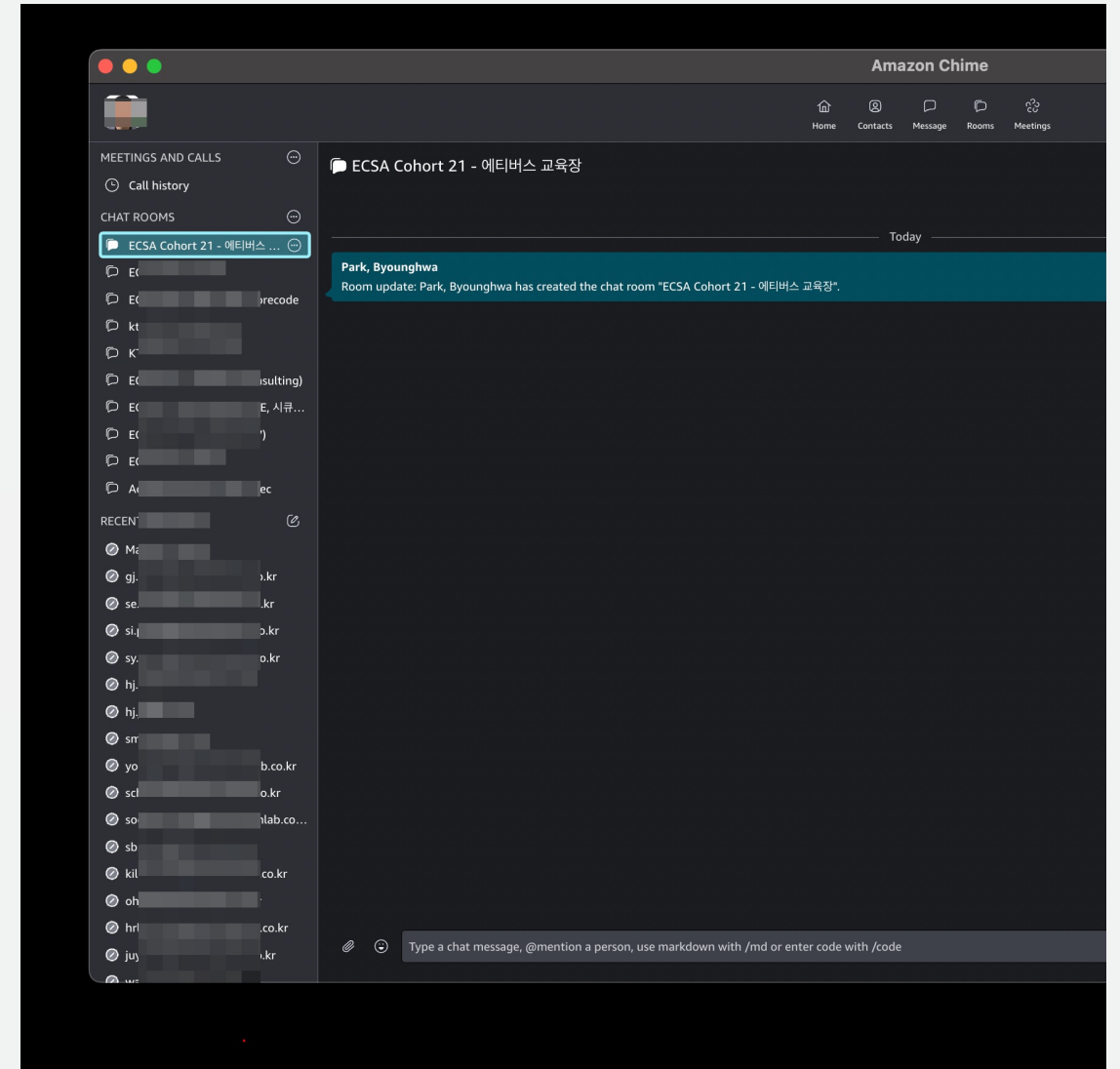
Amazon Chime은 애플리케이션 하나로 조직 내/외부에서 회의를 진행하고 채팅하고 업무상 전화 통화를 할 수 있게 해 주는 커뮤니케이션 서비스입니다.

Amazon Chime은 다음과 같은 기능을 제공합니다.

- HD 비디오, 오디오, 화면 공유, 회의 채팅, 전화 걸기 및 회의실 내 화상 회의 지원을 통해 온라인 회의를 시행하고 참석합니다.
- 채팅 및 채팅방을 사용하여 데스크톱과 모바일 디바이스에 걸쳐 커뮤니케이션을 지속합니다.
- Amazon Chime 관리 콘솔을 사용하여 기업 사용자를 관리하고 정책을 관리하며 SSO 또는 기타 고급 기능을 몇 분 안에 설정합니다.

Amazon Chime은 Windows, Mac, 웹, iOS, Android 디바이스에서 손쉽게 사용할 수 있는 앱을 제공합니다.

Amazon Chime: 만족도 높은 회의



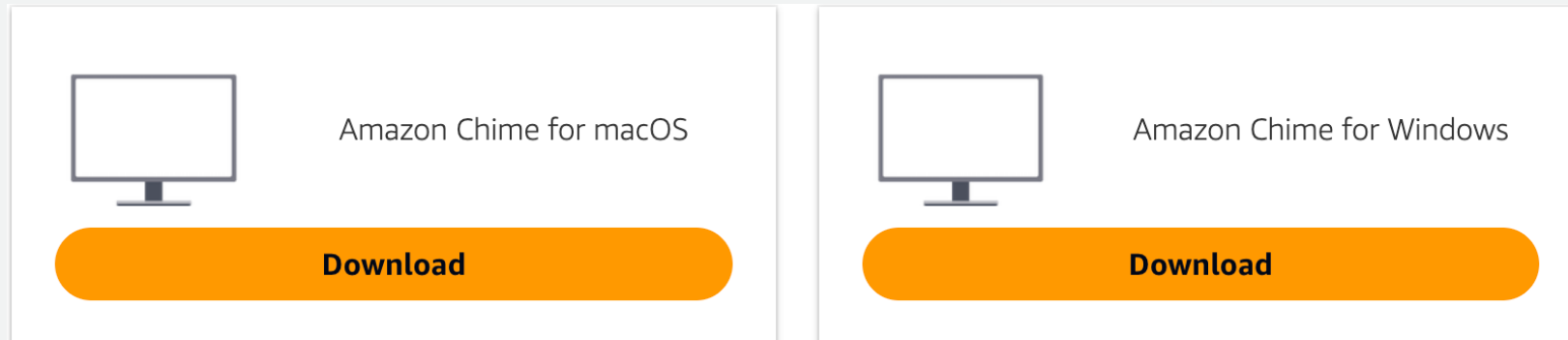
Communication Way

- Amazon Chime – 설정방법

1. 개인 이메일 수신 확인(수신된 메일이 안보이면, 스팸메일함 확인)

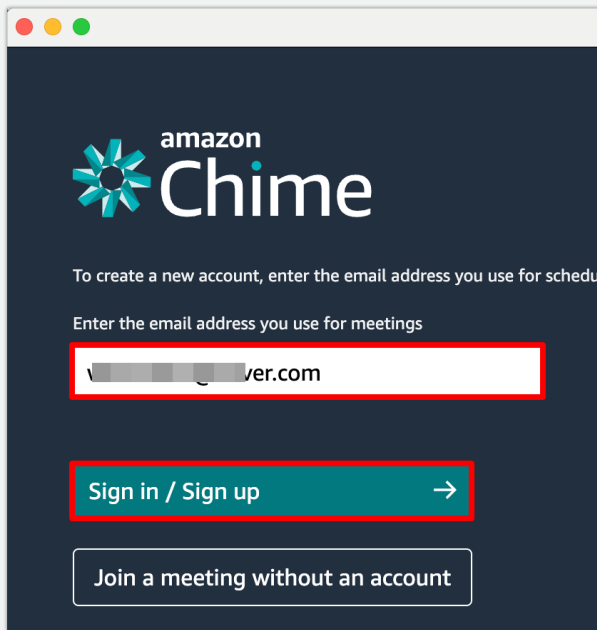


2. 다운로드 링크를 접속하여, Laptop OS에 맞는 Chime Client 다운로드

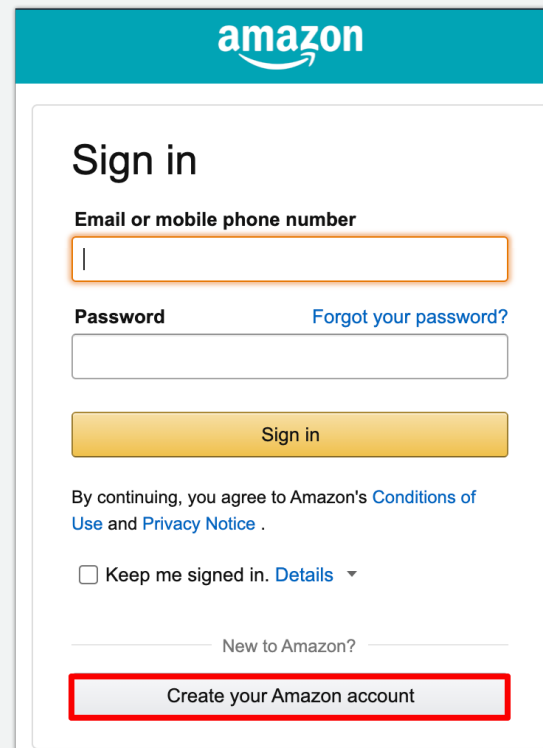


Communication Way

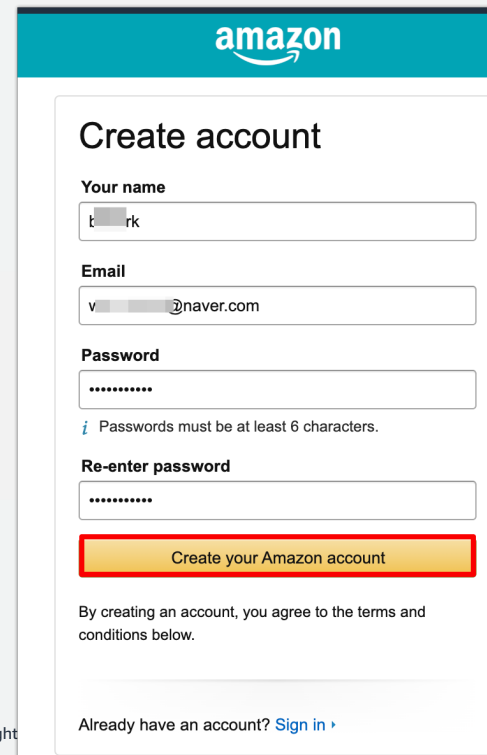
3. 만약, 계정이 이미 있다면, 메일 주소를 입력하고 로그인
4. 신규 가입시, 개인 이메일 주소 입력 후 Sing in / Sigh up 클릭
5. 입력한 Email로 OTP 입력하여 로그인 후 Chime 방 확인



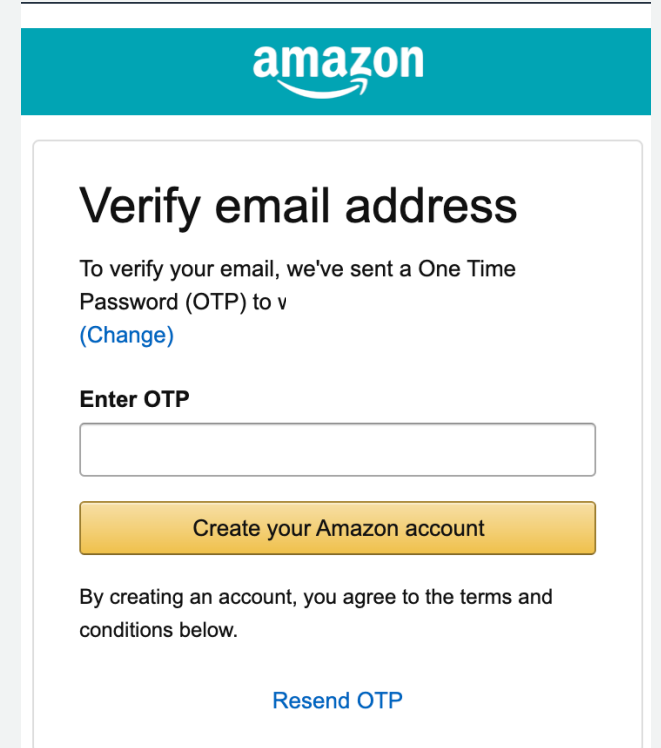
The screenshot shows the Amazon Chime sign-up page. At the top is the Amazon Chime logo. Below it, text says "To create a new account, enter the email address you use for scheduled meetings". A text input field for the email address is highlighted with a red rectangle. Below the field is a button labeled "Sign in / Sign up" with a right arrow, also highlighted with a red rectangle. At the bottom is a button labeled "Join a meeting without an account".



The screenshot shows the Amazon "Sign in" page. It has the Amazon logo at the top. The main heading is "Sign in". Below it are two input fields: "Email or mobile phone number" and "Password". The "Email" field is highlighted with a red rectangle. Below the password field is a "Sign in" button. A link "Forgot your password?" is next to the password field. Below the sign in section, there is a checkbox for "Keep me signed in" and a link to "Details". At the bottom, there is a link "New to Amazon?" and a button "Create your Amazon account" which is highlighted with a red rectangle.



The screenshot shows the Amazon "Create account" page. It has the Amazon logo at the top. The main heading is "Create account". Below it are three input fields: "Your name", "Email", and "Password". The "Email" field is highlighted with a red rectangle. Below the password field is a "Re-enter password" field. Below these fields is a "Create your Amazon account" button, highlighted with a red rectangle. A note says "Passwords must be at least 6 characters." Below the button, there is a link "Already have an account? Sign in".



The screenshot shows the Amazon "Verify email address" page. It has the Amazon logo at the top. The main heading is "Verify email address". Below it, text says "To verify your email, we've sent a One Time Password (OTP) to v". A link "(Change)" is next to the text. Below this is an "Enter OTP" input field. At the bottom is a "Create your Amazon account" button. A link "Resend OTP" is at the very bottom.

Q & A

Thank you!