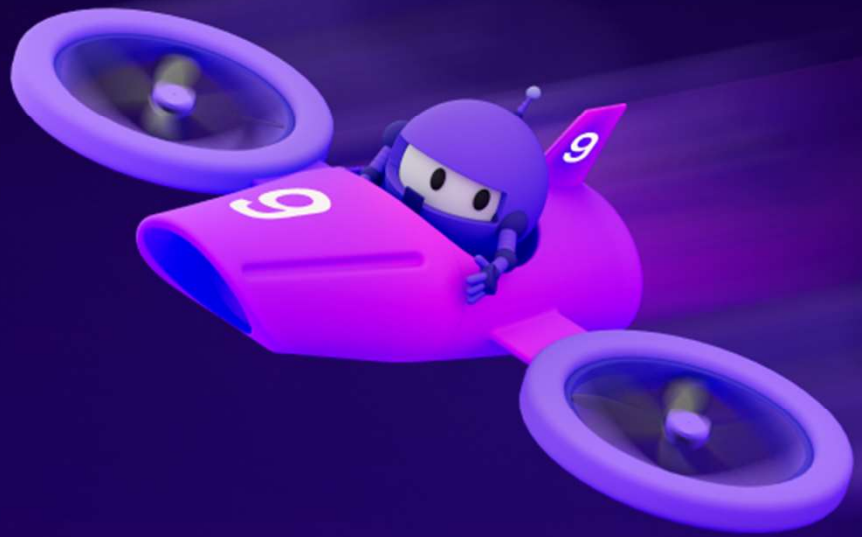
DotNetDevSecOps



닷넷데브 이상준

Agenda

01

개발자 배경을 가진
내가 DevSecOps로
팀을 옮긴 이유와
나의 비전

02

DevSecOps에 대한
개념 및 필요성

03

내가 맡았던 업무

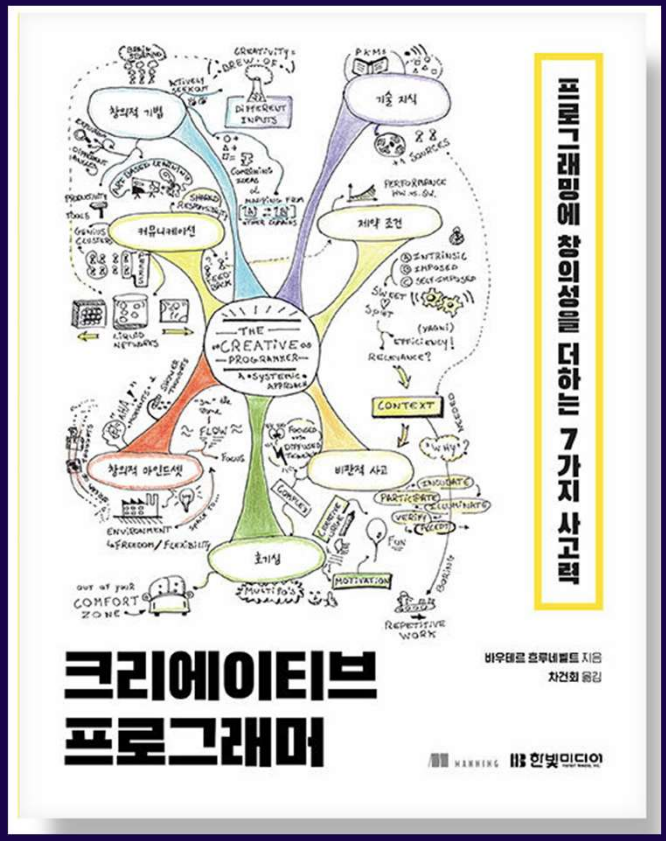
01

개발자 배경을 가진 내가 DevSecOps로 팀을 옮긴 이유와 나의 비전

창의적인 문제해결

크리에이티브 프로그래머

프로그래머의 창의성을 다룬 도서



8:08

편집

독서노트

p.31 2023.11.25

창의성에 대한 본질주의자들의 이러한 관점에는 많은 단점이 있습니다. 예를 들면 콘텍스트
context
, 즉 맥락을 완전히 무시합니다.

p.33 2023.11.28

어떤 것을 보고 다른 사람이 창의적이라고 말한다면 그것은 창의적입니다. 참 쉽죠? 창의성은 사회적 판단
social verdict
입니다.

p.37 2023.11.28

소프트웨어 개발 전문가들에게 “개발자로서 뛰어난 능력을 발휘하려면 어떤 비기술적 기술이 필요하다고 생각하나요?”와 같은 질문 방식으로 자체 조사를 실시한 적이 있습니다.
7
이러한 질문에 과연 어떤 대답이 나왔을까요? 바로 ‘창의성’입니다. 따라서 자신의 몸값을 높이고 싶다면 창의력을 발휘해야 합니다.

p.37 2023.11.28

창의적인 개발자로 살아야 하는 주된 이유

> 어떤 것을 보고 **다른 사람이 창의적이라고 말한다면** 그것은 창의적입니다. 참 쉽죠? 창의성은 **사회적 판단**(social verdict)입니다.

칼럼 제목: Advancing Creativity Theory and Research: A Socio-cultural Manifesto
학술지 출처: 2020년 9월 The Journal of Create Behavior

생각이 정리되었나요? 이제 앞의 질문에 대한 저의 대답을 알려드리겠습니다. 어떤 것을 보고 **다른 사람이 창의적이라고 말한다면** 그것은 창의적입니다. 참 쉽죠? 창의성은 **사회적 판단**social verdict입니다.[3] 여러분의 프로그래밍 노력이 창의적인 결과물로 이어졌는지는 여러분 자신이 아니라 여러분의 동료들이 결정합니다. 여러분의 결과물이 창의적이라고 여러분 스스로 결정할 수는 없습니다. 창의성은 사회문화적 현상이기 때문입니다.

3 Vlad Petre Glaveanu, Michael Hanchett Hanson, John Baer, et al. Advanced creativity theory and research: A socio-cultural manifesto. The Journal of Creative Behavior, 2020.

특정 그림을 천재적인 작품이라고 선언하는 미술 전문가들은 우리 같은 평범한 사람들의 의견을 좌지우지합니다(그림 1-1). 그들이 어떤 예술 작품이 위대하다고 평가하면 우리는 그 작품을 보고 경탄해 마지않지만, 왠지 의무감 때문에 그렇게 해야 할 것 같습니다. 만일 비평가들이 똑같은 그림을 보고 평범하며 흥미롭지 않다고 평가한다면 우리는 그 그림을 보려 하지 않을 것입니다. 아마 미술관 벽에 걸리지도 못하겠죠. 우리는 그림에 대한 전문 지식이 없기 때문에 해당 분야의 전문가에게 의존해야 합니다.

문제 해결력

전문 지식을 많이 쌓을 수 있는 방법

독서 및 인터넷 강의 수강

- 관심있는 주제에 대해서 저자에 의해 정제된 지식을 습득할 수 있다.
- 검색과 AI가 등장한 지금도 Step by Step으로 지식을 습득하기 위해 책, 사람이 직접 강의 해주는 것은 매우 효과적이다.
- 같은 책, 같은 강의를 익힌 사람들과 공감대를 형성하여 네트워킹을 할 수 있다.
- 확실한 방법이지만 시간이 오래 걸려서 중도 포기가 될 수 있다.
- 가성비가 떨어진다고 착각할 수도 있다.

검색엔진 활용

- 관심있는 주제를 검색하면 여러 글을 동시에 볼 수 있다.
- AI가 등장하기 전까지 최고의 방법이었으며, 현재도 자주 사용된다.
- 여러 검색된 글을 비교 분석해서 검증하기 까지는 옳은 지식인지 판단하기 어렵다.
- 내가 뭘 모르는지 몰라서 검색하기 어렵다.
- 주제에 대해 키워드마다 탐색이 들어가야 하는데 개인의 지적 호기심에 따라 얻을 수 있는 지식의 양이 다르다.

인공지능 활용

- 대충 질문해도 내가 뭘 알아야 하는지 가이드라인까지 잡아준다. 물론 자세하게 질문하면 답변도 잘해준다.
- 전혀 모르는 분야에 대해서도 인공지능과 함께라면 상당 부분의 업무 부담을 줄일 수 있다.
- 해줘~ 식으로 일해버릴 수가 있어서 사람이 나태해지거나 개인에 따라 이미 해결이 된 문제에 대해 Postmortem을 하지 않고 넘어가서 성장이 멈출 수 있다.
- 월간, 연간 구독료가 발생한다. 구독하는 유료 인공지능 서비스가 많을 수록 구독료가 증가한다.

제네럴리스트와 스페셜리스트

Generalist

Specialist

이미지 출처: ChatGPT DALL·E 3

거시적인
문제해결사

한 분야만 깊게 파는 것에도 장점이 있지만,
여러 분야를 두루 알면서
한 분야를 깊게 파신 분들의 디테일 적인 도움을 받아,
스스로 **판단하는 능력**을 지니게 되면
최고의 시너지가 아닐까?

안타까운 지능

잘할 사람은 어떻게 해서든 잘한다...

저를 구원해주신 팀장님 정말 감사드립니다...


龍が如く
TM


遊戯王
Yu-Gi-Oh!
MASTER DUEL

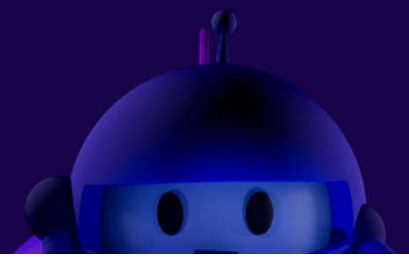

WORLD OF WARCRAFT
THE WAR WITHIN

단결의 힘

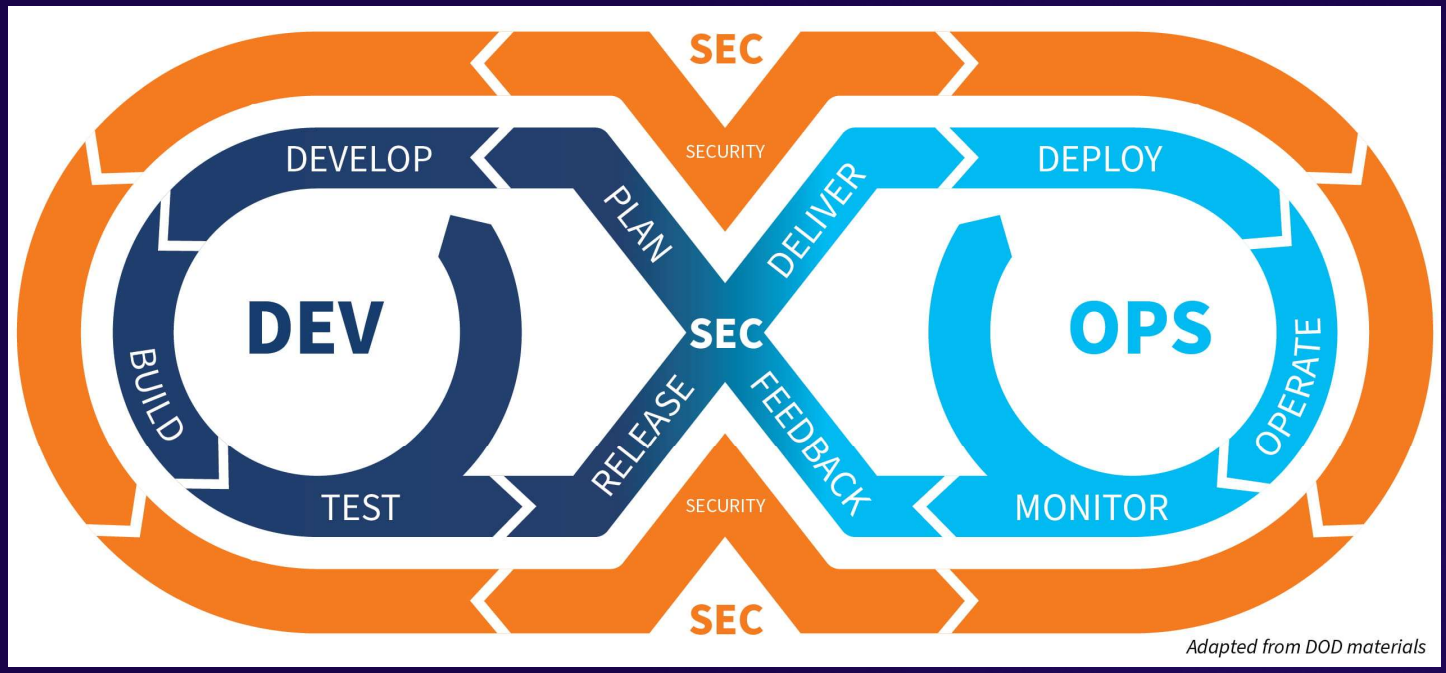
~~①: 장착 몬스터의 공격력 / 수비력은, 자신 필드의 앞면 표시 몬스터의 수 x 800 올린다.~~

좋은 협상이었다...

02
DevSecOps에 대한 개념 및 필요성



DevOps는 들어봤는데
DevSecOps는 뭐지?



출처: https://www.cohnreznick.com/insights/support-rapid-delivery-of-secure-software-with-devsecops

DevOps + Security

DevOps가 왜 필요한가?

효율성 증가

Jenkins, Github Actions, Ansible AWX,
Terraform etc.

비용 절감

인건비를 효율적으로 사용가능.

휴먼 에러 감소

실수를 하는 사람, 실수하지 않는 기계.
실수는 동물의 종족 특성.

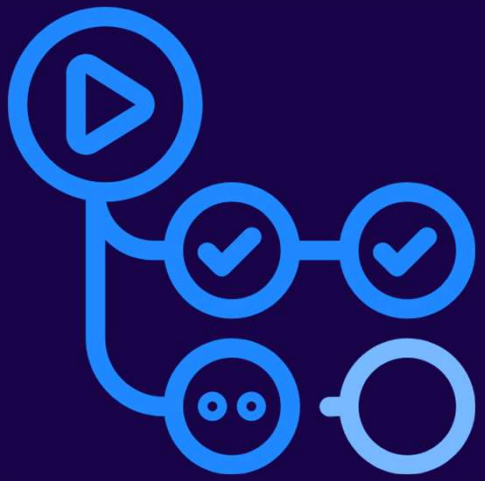
모니터링

파이프라인을 더욱 견고하게 보완 가능.

기계는 반복적인 일에 강하며 실수하지 않는다.

DevOps Tools

Jenkins



Github Actions

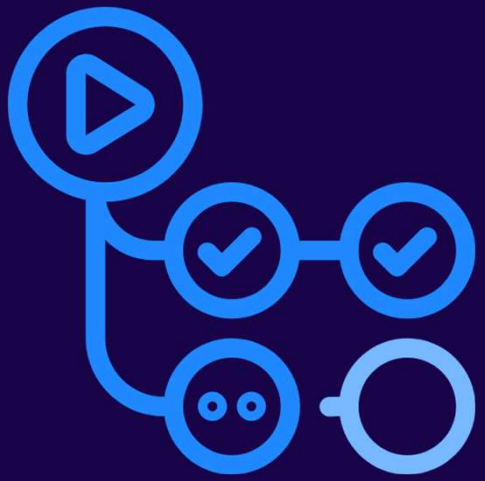
Ansible AWX

Terraform

Terraform vs Ansible AWX

DevOps Tools

Jenkins



Github Actions

Ansible AWX

Terraform

효율성 증가

파이프라인 정의

Ex) Jenkins, Github Actions, AWS CodePipeline, Jetbrains TeamCity etc.

비용 절감

인건비를 효율적으로 사용가능.

휴먼 에러 감소

실수를 하는 사람, 실수하지 않는 기계.
실수는 동물의 종족 특성.

모니터링

파이프라인을 더욱 견고하게 보완 가능.

기계는 반복적인 일에 강하며 실수하지 않는다.

이미지 출처: Instagram @creative_of_coding

효율성 증가

파이프라인 정의

Ex) Jenkins, Github Actions, AWS CodePipeline, Jetbrains TeamCity etc.

비용 절감

인건비를 효율적으로 사용가능.

휴먼 에러 감소

실수를 하는 사람, 실수하지 않는 기계.
실수는 동물의 종족 특성.

모니터링

파이프라인을 더욱 견고하게 보완 가능.

기계는 반복적인 일에 강하며 실수하지 않는다.

그럼 DevOps만 채용하면 문제가 해결되나?

업무 패턴화 비용

업무를 정확하게 단계별로 명시해야 함.
추상적이지 않고 소프트웨어 기준으로 세울 것.

담당자

DevOps 업무는 포지션이 따로 존재 할 만큼
많으므로 전담하는 직원 또는 팀 필요.

경험, 도메인 특성

DevOps는 담당자의 경험에 따라 인프라의 구축
형태가 차이가 있음.

어둠의 양산공장

~~①: 자신 묘지의 일반 몬스터 2장을 대상으로 하고 발동할 수 있다. 그 몬스터를 패에 넣는다.~~

자동화 및 효율이라는 문제해결을 위해 프로세스를 명시하는 것은 물리적으로 공장을 설계하고 건설하는 일과 유사하다.

업무 패턴화 비용

업무를 정확하게 단계별로 명시해야 함.
추상적이지 않고 소프트웨어 기준으로 세울 것.

담당자

DevOps 업무는 포지션이 따로 존재 할 만큼
많으므로 전담하는 직원 또는 팀 필요.

경험, 도메인 특성

DevOps는 담당자의 경험에 따라 인프라의 구축
형태가 차이가 있음.

고블린의 운영 실력

~~자신의 묘지에 존재하는 "고블린의 운영 실력"의 매수 + 1장을 덱에서 드로우하고, 패에서 카드를 1장 선택하여 덱의 맨 아래로 되돌린다.~~

어떤 경력의 DevOps 엔지니어가 운영하느냐에 따라 DevOps의 형태도 각기 다르다. 경력이 많다고 해서 반드시 좋지도 않고, 경력이 낮다고 해서 반드시 좋지도 않다.

만약 나열된 모든 문제를
해결했다면 더 이상 문제가 없을까?


Information Security

정보보호 법률 및 규정

법률 준수: GDPR, 개인정보보호법 등

인증 관리: ISMS

데이터 주권 관리: 데이터의 물리적 위치에 대한 법률적 판단

문서화: 보안 정책, 절차, 규정 준수 문서 작성

물리, 환경 보안

물리적 접근제어: 비 인가된 시설 이용 제한

자산 관리: 저장 장치 관리 및 보호

업무 공간 보안: 비밀번호 노트 및 메모 제거(사회공학적 해킹), 화면 잠금

조직 보안

보안 정책 수립: 비밀번호 정책, 접근제어, BYOD

보안 교육: 보안 의식 고양

사고 대응: 재해 복구 및 사고 대응 계획

사이버 보안

네트워크 보안: 방화벽, VPN, 침입 탐지, 백업 관리

어플리케이션 보안: OWASP Top 10, 코드 취약점 관리

데이터 보안: 데이터 암호화, 백업 관리

이미지 출처: https://skyvoice.org/sk/index.php?document_srl=25327

열려라 참깨!

단일 인증

- 문을 여는데 2FA 인증이 걸려 있지 않았다.

보안, 사고 대응 정책 없음

- 공개적인 장소에서 목소리로 외쳤기 때문에 다른사람이 쉽게 들을 수 있었다.
- 보안 의식이 부족해서 열러라 참깨 라는 비밀번호를 정기적으로 수정하지 않고 계속해서 사용했다.
- 사고 대응 정책 메뉴얼이 없어서 알리바바의 형도 알리바바가 다녀간 이후에 열려라 참깨를 외치고 동굴에 또 들어갔다.
- 강력한 비밀번호 생성 규칙이 없었다.

사회공학 해킹 취약

- 진짜인지는 모르겠지만 한국인으로서 익숙한 한국어 비밀번호를 사용해서 외우기 쉬웠다.

열려라 참깨!

가장 튼튼한 금고, 쉬운 암호

- 1940년대 미국의 원자폭탄 개발 프로젝트를 지휘한 미 육군 장군이 부임 첫날, 극비 문서를 보관할 금고를 보고 '당장 가장 튼튼한 금고로 바꾸라'고 호통을 쳤다.
- 그런데 1주일도 안 돼 비밀번호를 잊었다.
- 금고 업체 기사를 불렀더니 20분 만에 문을 열었다.
- 금고를 만들 때 기본 세팅된 비밀번호를 그대로 썼던 것이다.
- 현장에서 지켜보던 천재 물리학자 리처드 파인먼 박사가 "그런데 왜 20분이나 걸렸느냐"고 물었더니 "출장비를 받으려 적당히 시간을 때웠다"고 했다.

1q2w3e4r!@

- 냉전 시절 미국 지하 격납고에 저장된 핵미사일의 발사 비밀번호가 '00000000' 상태로 15년간 사용됐다는 사실이 뒤늦게 밝혀졌다.
- 1962년 국무장관이던 로버트 맥너마라가 사임한 뒤 비밀번호 때문에 미사일 발사가 늦어질까 걱정한 방공전략사령관이 비밀번호를 이렇게 바꿨기 때문이다.
- 글로벌 보안업체가 선정한 '최악의 비밀번호' 1위는 '12345'이다.
- 그런데 민간 해킹 단체 어나니머스가 시리아 독재자 알 아사드 대통령의 이메일을 해킹한 결과 '12345'를 비밀번호로 쓰고 있었다.

출처: [만물상] '비밀번호' 스트레스

보안은 평소에 잘해도 '딱 한번' 털리면 끝장

03
맡았던 업무 소개

인사 프로세스 점검

인사 데이터베이스의 정보를 활용하여
PowerShell을 통해 Active Directory 계정과 동기화

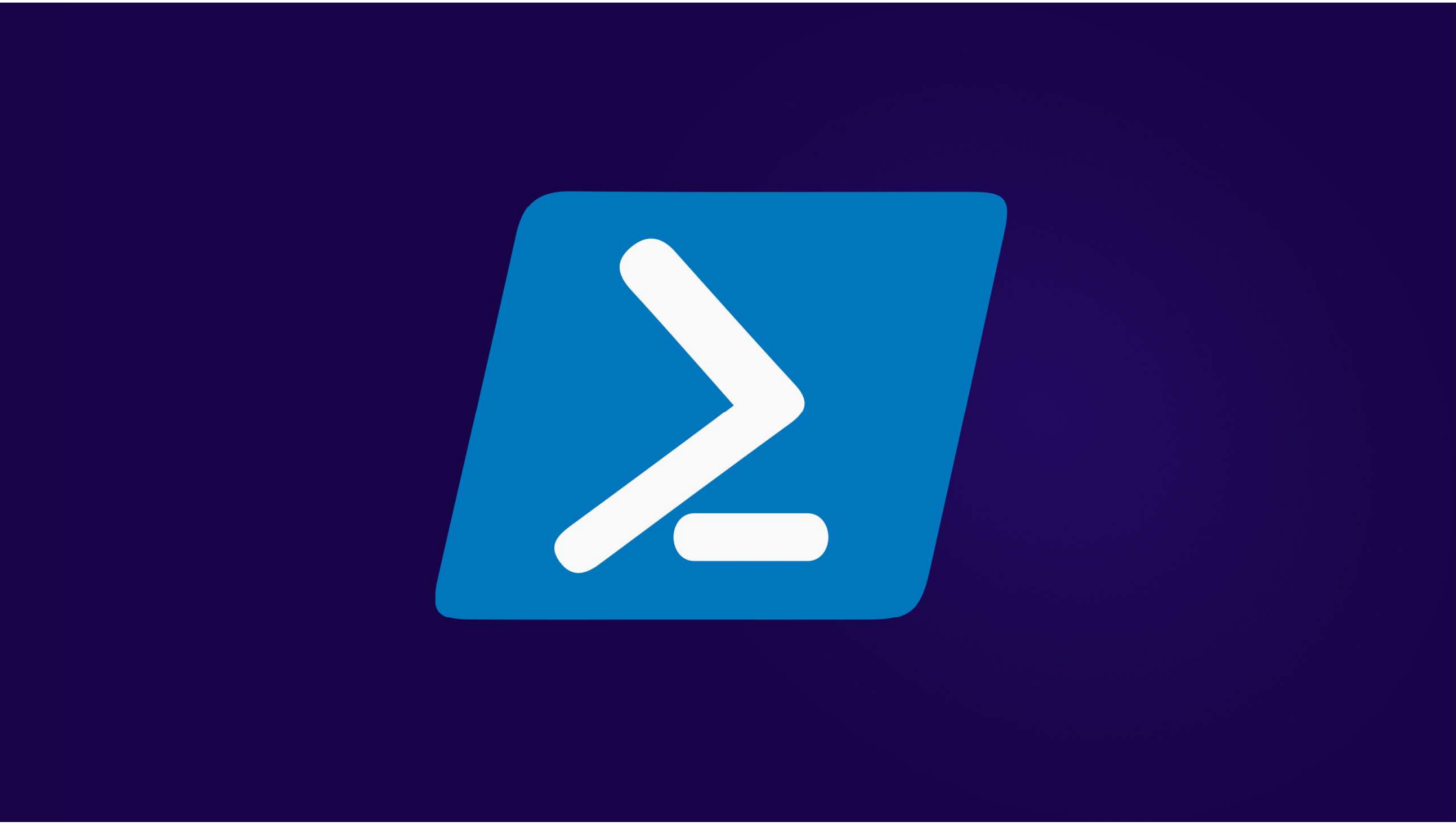

Microsoft
Active Directory

우리 회사는 Windows 안 쓰는데요?

+

Mobile Device Management(MDM) Solution

Bring Your Own Device(BYOD)

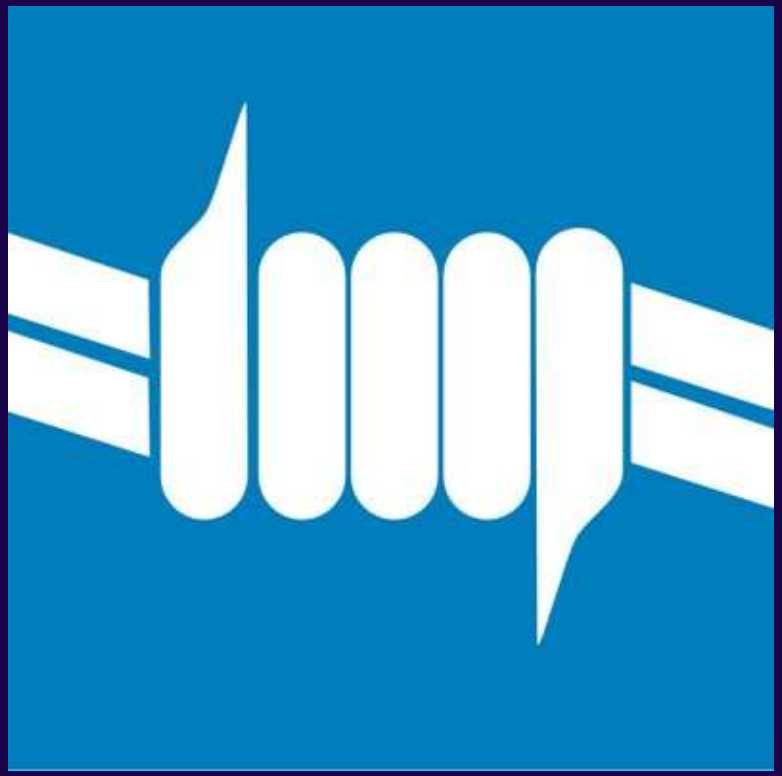


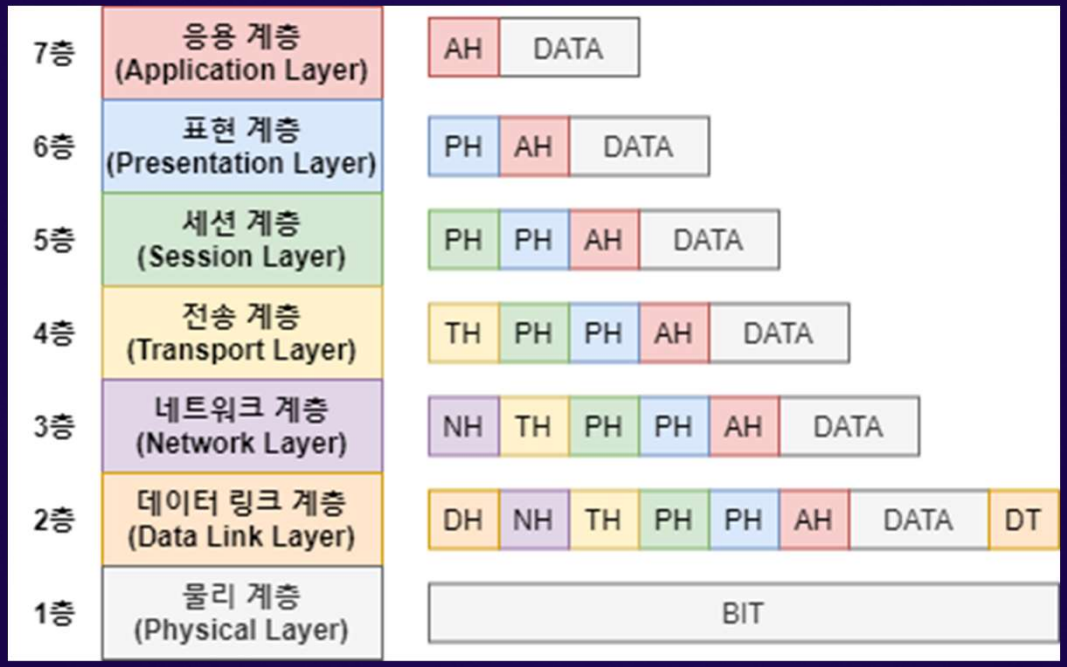
PacketFence

Open Source Network Access Control(NAC)

Active Directory 연계

IEEE 802.1x





이미지 출처: https://tgkim.com/posts/OSI-7-Layer/

GitLab 관리

On-Premise Git SCM 서버

기존 GitLab 서버를 유지보수 및 관리

신규 GitLab 설치 및 설정

On-Premise GitLab 관리

1

Linux Base

Linux에 패키지로 다운로드 하고
직접 설치 후 스토리지 mount

2

Network

내장 NGINX 또는 외부 NGINX
설정 과

3

Container Registry

내부 Container Registry의 포트
및 도메인 주소가 GitLab 자체의
주소와 섞이지 않아야 함.

AWS Lambda 개발

AWS Global Accelerator 포트 변경

.NET 환경에서 EC2 관련 AWS Lambda 개발 - ☁️ AWS 소모임 - 닷넷데브

시스템 비밀번호 갱신

다수의 Linux와 Windows 시스템의 비밀번호를 갱신 자동화

PowerShell, Crontab, Windows Task Scheduler

사내 스토리지 최적화

SHA256, MD5 중복체크

Avalonia UI

Helix Core 관리

기존 사내 Helix Core(Perforce) 관리

HelixCore

Helix Core 관리

기존 사내 Helix Core(Perforce) 관리

Thank you