정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

클라우드 환경의 서버 워크로드 보안 동향

박 문 형*, 김 대 협**, 한 현 상***, 이 용 준*

요 약

재택근무 확대와 온라인 수업 증가로 클라우드 환경으로의 전환이 확대되고 있다. 하지만 기존 온프레미스 환경과 달리 클라우드의 환경은 자원의 확장 및 재구성이 신속하기 때문에 복잡도가 증가 되었다. 본 논문에서는 급격히 전환되고 있는 클라우드 환경에서의 보안 위협과 이를 대응하기 위한 최근 위협관리 방안에 대해 분석하고, 특히 데브옵스와 같은 컨테이너 환경에서의 서버 워크로드 보안 동향과 수명주기 및 대응 자동화 등에 대한 구축 방향 관련 클라우드 환경 보안 동향을 연구한다.

Ⅰ. 서 론

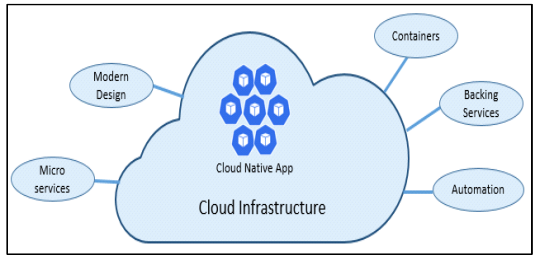
클라우드의 정의와 개념은 이미 10년 전부터 나왔지만, 최근 코로나로 인한 재택근무 확대와 온라인 수업 등으로 인한 폭발적인 수요 증가로 인해 클라우드로의 전환이 급격히 이루어지고 있다. 또한 코로나 이전, 국내 클라우드 환경 전환율은 10%가 되지 않았지만 이후 급격한 클라우드 환경으로의 전환이 가속화되고 있다.

[그림 1]과 같이, 클라우드로의 전환은 일반적으로 생각하는 리프트 앤 시프트(들어서 옮기는) 방식이 아니다. 온프레미스에서 사용했던 방식 그대로 사용한다면 보안적, 비용적으로 클라우드 전환의 이점이 줄어든다.

어플리케이션의 운영 방식도 데브옵스 형태로 통합하지 않으면 비용과 생산성 손실이 발생할 수 있다. 데브옵스의 툴과 프로세스가 반영되지 않은 어플리케이션의 운영은 빈번한 실수로 인한 막대한 비용이 초래될 수 있기 때문이다.

클라우드 전환의 이점을 최대한 활용하기 위해서는 클라우드 네이티브을 기반으로 마이그레이션이 필요하며 높은 유연성과 확장성을 가진 클라우드 서비스를 대응하고 처리하기 위해 데브옵스 형태의 통합 운영도 필요하다.

클라우드 네이티브 환경에서 동작되는 마이크로 서비스 및 컨테이너 서비스와 같이 오브젝트 단위로 동작되는 워크로드의 보호를 위해 전통적인 보안 솔루션으로는 대응이 불가능 하다[1]. 따라서 인프라 워크로드만 집중하여 많은 기능의 조합을 대응하기 위해 클라우드 환경의 위협을 식별하고 이에 대한 다양한 대응 전략이 필요하다[8].



〔그림 1〕 클라우드 네이티브 기본 핵심 요소

Ⅱ. 클라우드 보안 위협 현황 및 대응 동향

클라우드 환경은 관리를 자동화하여 자원의 확장과 재구성을 유연하게 하고 신속하게 함으로써 서버운영에 저비용·고효율을 제공하면서 빠르게 기술을 발전해 나아가고 있지만, 클라우드 환경의 복잡도가 증가함에 따라 이에 대한 보안 위협도 더불어 증가하고 있다[3]. [그림 2]는 클라우드 보안연합(CSA : Cloud Security allance)에서 2010년 클라우드 7대 보안위협을 발표하

* 극동대학교 과학기술대학 해킹보안학과 (강사, mhpark@kdu.ac.kr; 조교수, 2020032@kdu.ac.kr)
** 중앙대학교 융합보안학과 (대학원생, anonyges@cau.ac.kr)
*** Amazon Web Services사 Security & Risk Compliance팀 (Consultant, misadz@naver.com)

〔그림 2〕 CSA 클라우드 서비스의 보안위협 현황

였으며, 2019년에는 13대 보안 위협으로 확대되어 증가한 것을 확인할 수 있다[2].

2.1. 컴플라이언스에 따른 보안위협 관리

기술시장 분석 기관 가트너(Gatner)에 따르면 “클라우드 보안사고의 99%는 운영자의 설정 오류로 발생할 것”이라고 전망했다. 클라우드 환경은 개발과 배포 속도에서 이전보다 많은 발전을 이끌었지만, 끊임없이 변경되는 환경과 적은 인력 안에서 수 백개가 넘는 클라우드의 서비스 및 설정을 운영·관리하는 것은 어렵다. 또한, 퍼블릭 클라우드는 책임공유모델에 따라 서비스 사용자들도 컴플라이언스 등의 다양한 법규를 적용 받아 피해가 산정되면 손해배상의 책임이 발생하는데, 이러한 책임과 이슈를 효율적으로 해결하는 방법으로 CSPM(Cloud Security Posture Management) 솔루션을 사용한다.

CSPM은 컴플라이언스(Compliance) 또는 기업 보안 정책에 따라 클라우드 인프라의 위험 요소를 대응 및 예측하여 클라우드의 위험을 관리하는 솔루션이다. CSPM의 핵심 기능은 다음과 같다.

① 자주 변경되는 클라우드 환경에서 컴플라이언스의 정기적인 점검
② 다중 어카운트 및 멀티 클라우드 환경을 통합한 자산 가시성 제공
③ 컴플라이언스 위반이 발생 시 즉각 자동 대응

CSPM을 통해 자산의 가시성을 확보하고, 취약한 설정을 탐지하고 대응하면 설정 오류에 의한 보안사고를 사전에 방지할 수 있다.

2.2. 클라우드형 SaaS 서비스의 보안위협 관리

재택근무 및 온라인 수업 등의 영향으로 기업의 클라우드형 SaaS 서비스(CloudOne, Teams, workday 등)의 이용률이 증가하였다. 공식적으로 허가된 SaaS 서비스뿐 아니라 Shadow IT(IT/관리부서의 승인 없이 사용하는 비공식 애플리케이션) 사용률 역시 증가되었는데, 이런 환경 변화로 기존 보안시스템으로는 더 이상 업무를 보호할 수 없게 되었고, 다음과 같은 보안 문제가 발생하고 있다[6].

① 클라우드 간 발생하는 트래픽 모니터링 불가
② 비 구독 클라우드 앱에 대한 통제 불가
③ 악성코드·알려지지 않은 위협 탐지 불가

2019년에 발표된 사이버 인사이더에 따르면, 클라우드 서비스 사용에 따른 보안 이슈로 ‘데이터 유출위협’이라고 응답했을 만큼 SaaS 서비스 사용에 따른 데이터 유출 피해에 대한 걱정이 크다.[4].

CASB(Cloud Access Security Broker)는 클라우드 서비스 이용자와 클라우드 서비스 공급자에 구성되어 클라우드 사용에 있어서 안전을 보장해주는 중개자 역할을 제공한다. 기업이 사용하는 클라우드 및 애플리케이션에 대한 가시성 그리고 데이터 유출방지 및 컴플라이언스를 실현하는 서비스를 말한다. 따라서 클라우드 내 데이터에 대한 가시성을 제공하고, 이용자의 접근 통제를 적용함으로써 클라우드 자산을 보호하는데 목적이 있다. CASB는 다음과 같은 기능들이 있다.

① 데이터 유출방지 및 장치, 데이터 자산의 중요도에 따른 접근 제어 등 데이터 보호
② 업로드 및 다운로드 데이터 감지 및 알려진 및 알려지지 않은 위협을 탐지하는 위협 탐지
③ SSO 연동 및 취약 로그인 감시를 위한 다중 인증 지원
④ 어플리케이션 운영 관련, 가시성 제공

2.3. 데브옵스 환경의 보안위협 관리

전통적인 소프트웨어 개발과 운영은 별도의 전문영역이 있지만, 클라우드 환경에서 소프트웨어의 개발과 운영은 통합되거나 밀접한 연관성을 가진다. 클라우드로 전환하면서 많은 기업이 서버리스, 쿠버네티스 및 컨테이너 서비스 등을 사용할 수 있는 환경이 마련이

되었고 이러한 환경은 애플리케이션과 운영의 현대화를 가속하였다. 생각만 했던 인프라의 구성을 코드로 할 수 있게 됨으로써, 애플리케이션의 배포 속도가 비약적으로 향상되었다.

가트너는 “2022년까지 전 세계 조직의 75%가 컨테이터화된 응용프로그램을 운영하게 될 것(2019년:30% 미만)”으로 전망했다. 컨테이너에 대한 관심이 높아져서 많은 IT조직에서 빠르게 적용하고는 있지만, 컨테이너 보안에 대한 적용과 운영은 다소 부족한 것이 현실이다. 또한 취약한 컨테이너를 공격하는 사례가 빠르고 증가하고 있는데, 클라우드 네이티브 오픈소스 기술의 관리 단체인 CNCF(Cloud Native Computing Foundation)가 527개 기업을 대상으로 컨테이너의 관리 문제를 조사한 결과, “컨테이너 보안 운영”을 가장 큰 이슈로 선정하였다.[2]

컨테이너 보안을 위해서는 취약점 체크 및 코드 등 개발, 배포 및 운영까지 보호하는 개념의 확장이 필요하다. 워크로드 중심의 컨테이너 환경을 보호하기 위해 CWPP(Cloud Workload Protection Platform) 를 사용한다.

CWPP는 서버 워크로드를 보호하는데 사용하는 가트너에서 정의한 새로운 범주의 솔루션이다. 개발, 배포 및 운영까지 워크로드에서 보안을 구현하고 클라우드 네이티브 애플리케이션, 컨테이너 및 쿠버네티스에서 안정적인 클라우드 구성을 보장하기 위한 클라우드 형상 관리시스템이다.

상세 기능은 국내외 보안 벤더사에 따라 다르지만, 보통 컨테이너 등의 CI(Continuous Integration)/CD (Continuous Delivery) 파이프라인에 통합된 보안기능 제공으로 배포 단계 전에 이슈를 해결하고 네트워크 보안, 취약점 관리, 이상 행위 모니터링 등을 수행한다.[6]

Ⅲ. 클라우드 워크로드 보안 동향

가상화를 기반으로 하는 클라우드 환경은 물리환경과는 달리 워크로드를 중심으로 구현되어, 서버 위치를 식별하여 보안위협에 대응할 수 없다. 특히 수만 대에 이르는 가상화 서버를 운영하는 데이터센터에 워크로드가 어떤 시스템에서 가동되고 있으며, 어떤 시스템과 연관성이 있는지 파악하고, 가상화 자원의 생성과 변경 그리고 삭제와 같이 수명 주기에 따른 워크로드의 위험 식별과 자산의 가시성을 확보하는 것이 중요하다.

워크로드의 가시성은 주로 대시보드와 같이 모니터링이 가능해야 하며, 이를 통해 클라우드 보안사고를 예방하고 신속히 대응하는 차원으로 활용할 수 있다. 따라서 워크로드에 대한 가시성 확보하고, 보안시스템을 구축하는 것이 클라우드 보안의 가장 중요한 전략이다.[2]

3.1. 워크로드 보안 중심의 시스템 구축

워크로드 중심의 보안체계 구축에 대해서는 가트너에서 발표한 CWPP 솔루션을 사용한다.

[그림 3]과 같이, CWPP는 8개 계층으로 구분하여 워크로드 보안을 중심으로 한 전략을 제시하여 기업 환경에 적합한 보안전략을 선택하는 것이 중요하다.[7]

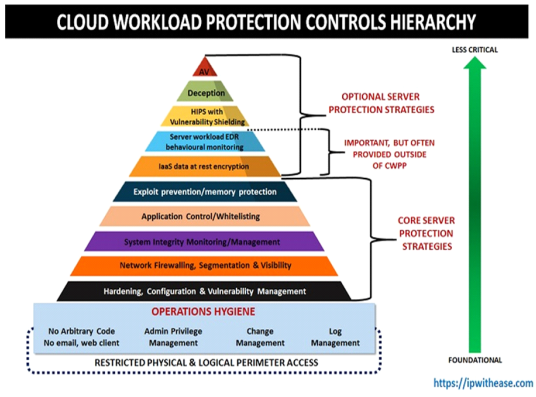
① Hardening, Configuration and Vulnerability Management : Telnet, FTP 등 불필요 서비스를 확인하여 제거하고, 취약점을 패치하여 시스템을 최신 보안 상태로 유지

② Network Firewalling, Visibility and Microsegemntation : 방화벽과 암호화를 통한 워크로드 격리, 시각화를 통해 워크로드의 가시성 확보, 마이크로세그먼트를 기반한 보안관리

③ System Integrity Assurance : 워크로드의 무결성 보증 및 실시간 모니터링

④ Application Control/White-Listing : 모든 어플리케이션을 차단, 필요한 파일 및 프로세스 만 허용하는 화이트 리스트의 기반의 보안 정책 구현

⑤ Exploit prevention/memory Protection : 악성코



〔그림 3〕 가트너의 CWPP 전략 8계층

드로부터 보호하기 위한 취약점 탐지·차단 및 메모리 보호 기능

⑥ Server Workload EDR, Behavioral Monitoring and Threat Detection/Response : 클라우드 환경에서 엔드포인트 보안 강화 및 행위 기반의 위협 탐지 및 대응

⑦ Host-Based IPS With Vulnerability Shielding : 호스트 및 컨테이너 간 내부 취약점 공격을 차단할 수 있는 침입방지솔루션

⑧ Anti-malware Scanning : 퍼블릭 클라우드 환경에서 악성코드 탐지와 차단에 사용

국내외 서비스 되고 있는 CWPP 솔루션은 [그림 4]와 같이 8가지 기능을 모두 제공하는 솔루션이 있지만 그 수는 적으며, 솔루션 대부분이 그 일부 기능만 제공하고 있다[5].

클라우드 시장 성장과 함께 CWPP 시장 역시 높은 성장이 예상된다. IDC 자료에 따르면, CWPP의 시장 규모는 9억 7,100만 달러로 집계되었다. 또한 가트너 역시 2023년까지 지속적으로 19% 이상 성장할 것으로 전망했다.

현재까지는 글로벌 기업이 CWPP 솔루션 시장에서 독점적이다. 트렌드마이크로가 강세를 보이고 있으며 이외에 브로드컴(시만텍)과 맥아피가 선점하고 있다. 이외에 팔로알토네트웍스, 체크포인트 등이 CWPP 솔루션을 제공하고 있다.

CWPP 시장의 특징은 백신(안티바이러스) 솔루션을 제공하던 기업들이 그 기술을 기반으로 높은 점유율을 보이고 있다는 점이다. 대표적으로 백신을 제공했던 기업인 브로드컴(시만텍), 맥아피, 소포스 등을 들 수 있고, 국내의 경우, 안랩이 시장에 제품을 출시하여 솔루션을 제공하고 있다.[5]

공간 노출 영역 축소 실행 전 보호 실행 후 보호

CWPP의 핵심 기능	CWPP 범위						
	전체 영역	컨테이너	서버리스	메모리, 프로세스 무결성 보호	네트워크와 마이크로세그멘테이션	EDR	취약성, 건고화 및 구성 컴플라이언스
건고화 및 구성							
호스트 기반 네트워크 방화벽							
마이크로세그멘테이션							
이용방지 및 메모리 보호							
취약성 점검							
어플리케이션 통제							
특권 계정 관리							
안티바이러스							
취약점 차폐							
무결성 통제							
사용자 행동 모니터링							
침입 탐지/예방							
워크로드 EDR							
자동 복구							

〔그림 4〕 CWPP 종류와 기본 기능

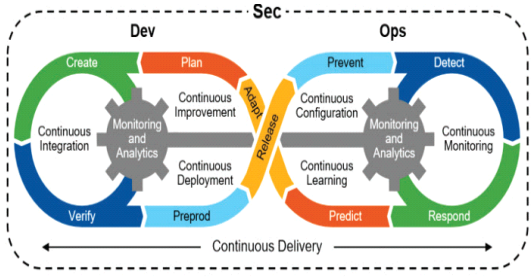
3.2. 애플리케이션 수명 주기에 따른 보안 체계

클라우드 환경에서는 애플리케이션을 개발하고 운영하는 방식이 이 전보다 급진적으로 변화되고 있다. IT환경의 경쟁력은 신속한 개발과 배포이며, 이에 부합하는 데브옵스(DevOps)가 현재 자리 잡고 있다.

데브옵스는 개발과 운영으로 구분되는 전통적인 방식에서 벗어나, 개발팀과 운영팀과 협업을 최적화하거나 통합함으로써 애플리케이션 수명 주기 전체에 빠르고, 안정적인 운영 서비스를 제공할 수 있다. 그리고 데브옵스는 접근 방식의 신속성과 대응 방법을 최대한 활용하기 위해서 보안 역할도 애플리케이션 수명 주기 전반에 걸쳐 개발와 운영에 통합해야 한다는 필요성 역시 제기되었다. 이에 따라 데브옵스에 보안이 결합되어 데브섹옵스(DevSecOps)라는 용어가 나오게 되었다.

[그림 5]와 같이, 데브옵스에서의 보안 역할은 개발이 완료된 후에 수행했으나, 데브섹옵스와 같이 개발단계부터 보안을 고려하지 않으면 취약점을 점검하기 어렵고 심각한 취약점이 발견되면, 개발부터 배포까지 처음부터 다시 수행하여야 하여 시간과 노력이 많이 소요된다. 운영단계에서도 보안설정 오류를 점검하지 못해 심각한 보안사고가 발생할 수도 있다.

애플리케이션의 생명 주기 전체에 보안 기능을 고려하지 않는 경우, 클라우드 네이티브의 신속성을 저해할 수도 있으며, 더불어 중요 정보가 유출되는 등 보안사고로 이어져 해당 업무 자체에 대한 신뢰가 무너지는 결과가 발생할 수 있다.



〔그림 5〕 데브섹옵스(DevSecOps) 수명 주기

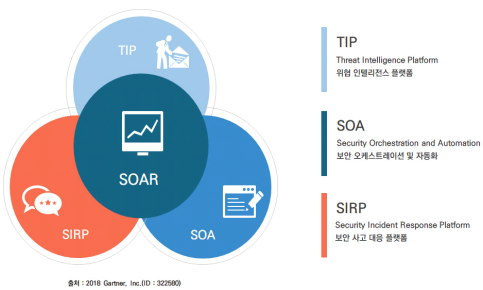
3.3. 지능화된 대응체계 구축

기존 보안시스템은 한정된 인력으로 24시간 사이버 공격을 대응하는 방법으로, 고도화된 사이버공격과 다양한 운영 환경 및 인력 부족 등의 원인으로 클라우드 보안 환경에서는 운영이 어렵다. 따라서, 지능화된 보안시스템을 운영하기 위해서는 사람의 판단기준을 중심으로 하는 기존 방식에서 벗어나, 인공지능과 머신러닝과 같은 최신 기술을 사용하여 학습하고, 대용량으로 발생하는 사이버공격에 대한 대응을 자동화하는 방향으로 발전하여야 한다.

[그림 6]은 자동화를 통해 반복적인 업무를 줄여주는 보안 오케스트레이션(SOA)과 자동화 영역과 보안사고 발생 시 정해진 프로세스에 따라 대응체계를 자동화하는 보안사고 대응 플랫폼(SIRP) 및 여러 보안 요소들에서 위협 데이터를 수집, 연관 분석을 수행하고 기존 보안시스템과 연계를 통해 위협에 대한 대응력을 높일 수 있는 위협 인텔리전스 플랫폼(TIP)을 통합한 것이 보안 운영 자동화 및 대응(SOAR : Security Orchestration, Automation and Reponse)이다.

특히, 클라우드의 전환은 가상화 자원의 확대, 횡단(East-West) 트래픽의 증가 및 호스트 내부로의 침해 확대, 멀티 클라우드, 마이크로 서비스 등 클라우드 환경의 특수성으로 인해 위협 요소가 증가하고 있으며 컴플라이언스는 복잡해지고 있다. SOAR는 클라우드 환경에서 보안 운영 자동화, 지능형 위협 탐지 및 대응을 위한 솔루션으로 필요성이 대두되고 있다.

신종 악성코드와 취약점이 하루 수천 건씩 발표되고 있는데 전통적인 분석 방법으로는 지능형 공격을 신속하게 대응할 수 없다. 효과적으로 대응하기 위해 공격기법을 분석하는 것보다 베이스라인을 산정하여 기준을 정립하는 것이 필요하다. 정상적인 서비스 상태를 특정하고 산정된 기준값에서 벗어나는 이상행위를 식별하고 대응할 수 있는 이상행위 탐지 기반의 대응시스템 구축이 필요하다.



〔그림 6〕 SOAR (TIP+SOA+SIRP)

Ⅳ. 결 론

클라우드 보안은 전통적인 온프레미스 방식의 보안 방식과는 달라진다. 기본 방식은 사람 중심 보안이였지만 클라우드에서는 머신러닝이나 인공지능이 판단하고 자동화 처리되는 대응 시스템으로 변화되고 있다.

클라우드 보안은 복잡하며 기존 보안 아키텍처에 대한 많은 영향을 미치지만, 클라우드 공급자들과 클라우드 보안 솔루션은 계속 발전하고 있다. 클라우드 보안 솔루션이 제공하는 기능은 다음과 같다.

① CSPM 솔루션의 기능
- 자동화된 보안 스캐닝과 복원
- 클라우드 침입의 가장 큰 원인인 고객의 잘못된 구성을 방지
- 클라우드 서비스 운영 모니터링

② CWPP 솔루션의 기능
- 컨테이너와 VM을 위한 보호
- 네트워크 분할 정책 생성과 모니터링
- 워크로드 구성 관리
- 시스템 건정성 확인

CWPP 솔루션의 최근 경향은 CSPM 등 다른 보안 솔루션과의 연계를 강화하고 있다는 점이다. 해외 기업뿐만 아니라 국내 기업들도 CSPM의 일부 기능을 통합하고 있고 더불어 통합관리 할 수 있는 플랫폼을 제공하여 사용 편의성을 높이고 있다. 대부분 CWPP로 시작했지만 CSPM과 결합하여 발전하기도 하고 필요한 핵심요소만 결합하여 플랫폼화하여 발전 중이다.

참 고 문 헌

[1] Microsoft Inc, “클라우드 네이티브 정의”, https://docs.microsoft.com/ko-kr/dotnet/architecture/cloud-native/definition

[2] 문용식, “클라우드의 미래모습과 보안”, 한국지능정보사회진흥원, pp.26~31, Dec. 2020.

[3] 우지영, 노경란, 권오진, “2014 KISTI 미래유망기술 10선 : 클라우드 환경 보안“, 한국과학기술정보연구원, 2015.

[4] CLOUD INSIGHT, “클라우드 보안, 9개 키워드로 완벽 정복 Part_2,” BESPIN GLOBAL, 2020.
[5] 권정수, 컴퓨터월드, “클라우드 보안의 첫걸음, CWPP“, ITDAILY, Aug. 2020.
[6] 김형주, 인포섹 공식 블로그, “클라우드 보안, 완벽한 적용을 위한 개념 3가지!”, https://m.blog.naver.com/skinfosec2000/222083410400, 8. Sep. 2020.
[7] McAfee Inc, “What Is a Cloud Workload Protection Platform(CWPP)” https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-cwpp.html
[8] Redhat Inc, “클라우드 네이티브 애플리케이션 구현을 위한 과정”, eBook, 2018.

〈저 자 소 개〉

박 문 형 (Moonhyung Park)
2003년 8월 : 강원대학교 경영대학 경영학사
2008년 8월 : 건국대학교 정보통신대학원 정보보호학 공학석사
2019년 3월~현재 : 극동대학교 해킹보안학과 강사
<관심분야> 클라우드 보안, 엔드포인트 보안, 정보보안

김 대 협 (DaeHyeob Kim)
2017년~현재 : 중앙대학교 융합보안학과 석사과정
2020년~현재 : Fortinet Korea SE팀 Consultant
<관심분야> 클라우드, 정보보호, 인공지능

한 현 상 (HyeonSang Han)
2019년 2월 : 성균관대학교 정보통신대학원 정보보호학 공학석사
2020년~현재 : Amazon Web Services사 Security & Risk Compliance 팀 Consultant
<관심분야> 클라우드, 침해사고 대응, 네트워크 보안

이 용 준 (Yongjoon Lee)
1999년 2월 : 강남대학교 전자계산학과 공학사
2001년 2월 : 숭실대학교 컴퓨터공학과 공학석사
2005년 2월 : 숭실대학교 컴퓨터공학과 공학박사
2020년 4월~현재 : 극동대학교 해킹보안학과 조교수
<관심분야> 클라우드, 보안관제, AI·사이버보안 융합