정 보 보 호 학 회 지
제34권 제3호, 2024. 6

제로트러스트 성숙도 진단, 도입계획 수립, 도입효과 측정을 위한 공격자 관점의 접근

이 철 호*, 최 창 진**, 정 시 헌***, 곽 진****

요 약

제로트러스트 도입을 검토하고 있는 조직은 제로트러스트를 구성하는 6개 핵심요소에 대한 자신의 성숙도 수준을 측정하여 목표 수준과의 차이를 식별한 후, 목표 성숙도 수준 달성을 위한 제로트러스트 도입계획을 수립하고, 도입 후 목표 성숙도 수준의 달성정도를 정량적으로 확인할 수 있어야 한다. 이를 위한 접근법 또한 제로트러스트의 기본철학(Never Trust, Always Verify)을 준수해야 하므로, 가장 효과적인 방법은 공격자 관점의 침투시험(Penetration Test, 모의해킹)을 도입하는 것이다. 본 연구는 침투시험을 기반으로 제로트러스트 핵심요소별 성숙도를 측정하는 방법과 제로트러스트 도입 전후 보안성 향상 정도를 정량적으로 측정하는 방법을 제시한다.

Ⅰ. 서 론

2023년 국내에서 발간된 제로트러스트 가이드라인 1.0은 제로트러스트의 6개 핵심요소 및 3단계 성숙도 모델, 제로트러스트 도입 등에 관한 기본원칙을 제시하고 있다[1]. 그러나, 제로트러스트 보안모델을 도입하고자 하는 수요자(기관 및 기업) 입장에서는 자신의 현재 보안수준(제로트러스트 6개 핵심요소별 성숙도 등)을 객관적으로 측정하고 비용 효과적인 제로트러스트 도입을 위한 구체적인 방법론 및 도구가 필요하며 이에 대한 다양한 관점의 연구와 실증이 요구된다.

본 연구는 공격자 관점의 침투시험을 기반으로 제로트러스트 성숙도를 측정하는 방법론을 제안하고, 이를 토대로 제로트러스트 도입에 관한 세부적인 가이드라인을 마련하고자 하는 노력을 소개한다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련된 기술적 배경을 소개하고 3장에서는 제로트러스트 성숙도 진단, 도입계획 수립, 도입효과 측정을 위한 침투시험 기반의 방법론을 제안한다. 4장에서는 추가적인 고려사항 및 수요자 관점의 요구사항을 정리한 후 5장 결론을 끝으로 마무리한다.

Ⅱ. 배 경

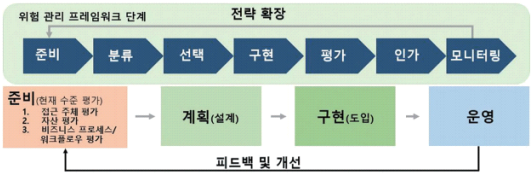
본 장에서는 제로트러스트 도입을 위한 절차와 도입과정에서 핵심 척도가 되는 성숙도 모델을 소개한다. 그리고, 제로트러스트 성숙도를 측정하기 위한 공격자 관점의 방법론으로 PTaaS(서비스형 침투시험)와 BAS(Breach and Attack Simulation)을 소개한다.

2.1. 제로트러스트 도입을 위한 절차

조직의 상황에 맞는 제로트러스트를 도입하기 위해서는 현재 상황을 분석하고 반영하는 도입계획 수립이 필요하며, 조직의 자산에 대한 보안위협을 줄이기 위한 절차로서 위험관리 프레임워크와 연계가 가능하다[1][5][6].

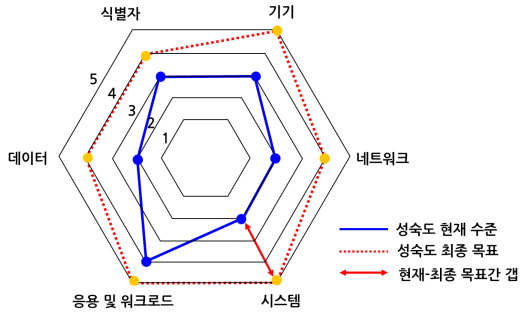
준비단계에서는 제로트러스트를 도입하기 전에 기업망 핵심요소를 중심으로 조직의 현재 제로트러스트 성숙도 수준에 대한 평가를 실시한다. 계획단계에서는

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2024-00331950, 차세대 지능형 교통시스템(C-ITS) 취약점 검증 및 사이버공방훈련 기술개발)
* 아주대학교 국방디지털융합학과(NCW학과) (박사과정), ㈜엔키화이트햇 (연구소장, chlee@enki.co.kr)
** 가천대학교 정보보호학과 (박사과정), ㈜엔키화이트햇 (MDR팀장·이사, cjchoi@enki.co.kr)
*** ㈜엔키화이트햇 (컨설팅팀장, shjeong@enki.co.kr)
**** 아주대학교 사이버보안학과 (교수, security@ajou.ac.kr)



〔그림 1〕 제로트러스트 도입을 위한 세부 절차〔1〕〔5〕〔6〕

6개 핵심요소별 평가된 성숙도 수준을 기반으로 조직이 목표로 하는 성숙도 수준을 설정하고, 현재와 목표 사이의 차이(Gap)를 식별하여 도입계획을 수립한다. 이후, 관련 정책, 기술, 솔루션 등을 도입한 후 제로트러스트 성숙도를 다시 측정하여 목표 성숙도 달성여부를 판단하고 개선방안을 도출하여 지속적으로 성숙도 수준을 고도화한다.



〔그림 2〕 제로트러스트 성숙도 목표 다이어그램〔1〕

2.2. 제로트러스트 성숙도 모델

상기 제로트러스트 도입절차에서 살펴본 바와 같이, 준비단계 및 피드백·개선 단계에서 조직의 제로트러스트 성숙도를 측정해야 하므로, 성숙도 모델과 이에 대한 측정 방법은 제로트러스트 도입에 있어서 핵심적인 역할을 하게 된다.

〔표 1〕 제로트러스트 성숙도 단계〔1〕

구분	주요 내용
기존 (Traditional)	아직 제로트러스트 아키텍처를 적용하지 않은 수준으로, 대체로 네트워크 방어에 초점을 맞춘 경계 기반 보안모델이 적용되어 있는 상태(정교한 공격, 내부자 공격 등에 일부 취약성을 가짐)
향상 (Advanced)	제로트러스트 철학을 부분적으로 도입한 수준으로 제로트러스트 원칙이 보안 아키텍처에서 핵심 기능이 되는 상태(최소 권한 접근, 네트워크 분할, 로깅 및 모니터링 등이 부분적으로 적용되어 기본보다 높은 보안성 달성)
최적화 (Optimal)	제로트러스트 철학이 전사적으로 적용된 상태(자동화된 운영, 네트워크 세분화, 신원에 대한 지속적인 검증을 통한 최소 권한의 안전한 접근제어 등을 통하여 보안성이 크게 개선)

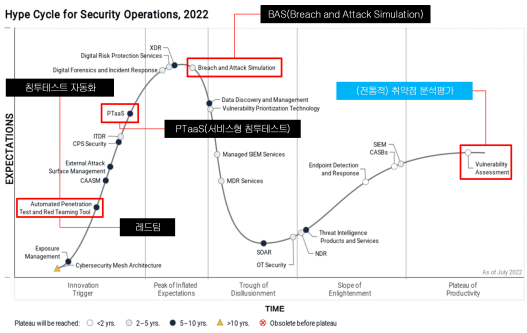
표 2에서 나타내는 각 기능에 대해 표 1에서 제시되는 3단계(기존, 향상, 최적화) 성숙도가 적용된다.

〔표 2〕 제로트러스트 핵심요소별 기능〔1〕

핵심요소	기능
식별자·신원 (Identity)	식별자 관리
	인증
	위험도 평가
	가시성 및 분석
	자동화 및 통합
기기 및 엔드포인트 (Device/Endpoint)	정책 준수 모니터링
	데이터 접근제어
	자산 관리
	가시성 및 분석
	자동화 및 통합
네트워크 (Network)	네트워크 세분화
	위협 대응
	암호화
	가시성 및 분석
	자동화 및 통합
시스템 (System)	접근통제
	시스템 계정 관리
	네트워크 분리 정책
	시스템 보안 및 정책 관리
	가시성 및 분석
	자동화 및 통합
응용 및 워크로드 (Application & Workload)	접근 인가
	위협 보호
	접근성
	응용 보안
	가시성 및 분석
	자동화 및 통합
데이터 (Data)	데이터 목록 관리
	접근 결정방법
	암호화
	가시성 및 분석
	자동화 및 통합

2.3. 공격기술 기반의 취약점 분석평가 기술

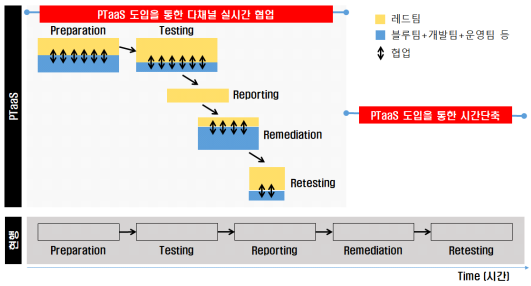
2022년 Gartner가 발간한 Hype Cycle for Security Operations에 따르면, PTaaS(서비스형 침투시험), BAS(Breach and Attack Simulation), 레드팀 자동화 등 공격기술 기반의 취약점 분석평가 기술이 등장하여 전세계적으로 주목받고 있다[7].



〔그림 3〕 Gartner, Hype Cycle for Security Operations 2022〔7〕

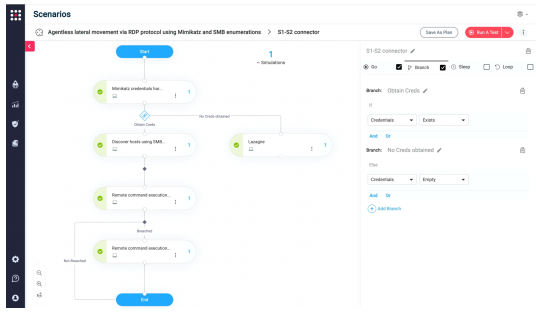
인력에 의존적인 기존 침투시험(모의해킹)의 한계를 극복하고 속도향상, 확장성, 커버리지, 지속시험, 비용효과성 등의 장점을 얻기위한 서비스형 침투시험(PTaaS: Penetration Test as a Service) 등의 자동화 방법론이 등장했으며, 향후 5~10년내에 시장에서 정점에 위치할 것으로 전망된다.

PTaaS는 블루팀, 개발팀, 운영팀, 레드팀이 다채널 협업을 통해 제품개발 과정의 DevOps체인에 침투시험을 결합하는 서비스형 침투시험 모델이다.



〔그림 4〕 서비스형 침투시험(PTaaS) 도입효과

BAS는 조직내에서 침투테스트 프로세스를 자동화하고 지속적으로 수행하는데 유용하며 화이트해커와 같은 독창성은 갖지 못하지만 다양한 종류의 공격TTP를 시험할 수 있으며, 상용 제품군은 전세계적으로 AttackIQ, SafeBreach 등이 있고 오픈소스는 MITRE Caldera, Atomic Red Team 등이 있다.



〔그림 5〕 美 SafeBreach社 No-Code RedTeam

상용 BAS 제품은 다양한 공격 TTP를 조합하여 APT 공격 시나리오를 구성할 수 있으며, 특정 공격 TTP에 대해서 연관된 위협관리프레임워크(RMF)의 통제항목을 매핑하여, 조직이 해당 공격(위협)에 대응하기 위해 집중해야 할 통제항목을 선정하도록 가이드를 제시한다.

이와 같은 PTaaS, BAS 등의 공격기술 기반 침투시험 기술을 이용하면 제로트러스트 핵심요소 및 기능에 대한 성숙도 수준을 객관적으로 측정할 수 있을 것으로 기대된다.

Ⅲ. 제로트러스트 핵심요소별 성숙도 진단, 도입계획 수립, 도입효과 측정을 위한 침투시험 기반의 방법론

본 장에서는 제로트러스트 핵심요소별 성숙도 모델을 기준으로 MITRE ATT&CK 기반 침투시험 시나리오를 수립하고, 이를 이용한 성숙도 측정 방법과 도입효과 측정 방법을 제안한다.

3.1. 제로트러스트 핵심요소별 성숙도 측정을 위한 MITRE ATT&CK 기반 침투시험용 공격TTP 선정

제로트러스트의 기본철학(Never Trust, Always Verify)을 준수하면서 제로트러스트 성숙도를 측정하기 위해서는 공격자 관점의 침투시험이 적합하다.

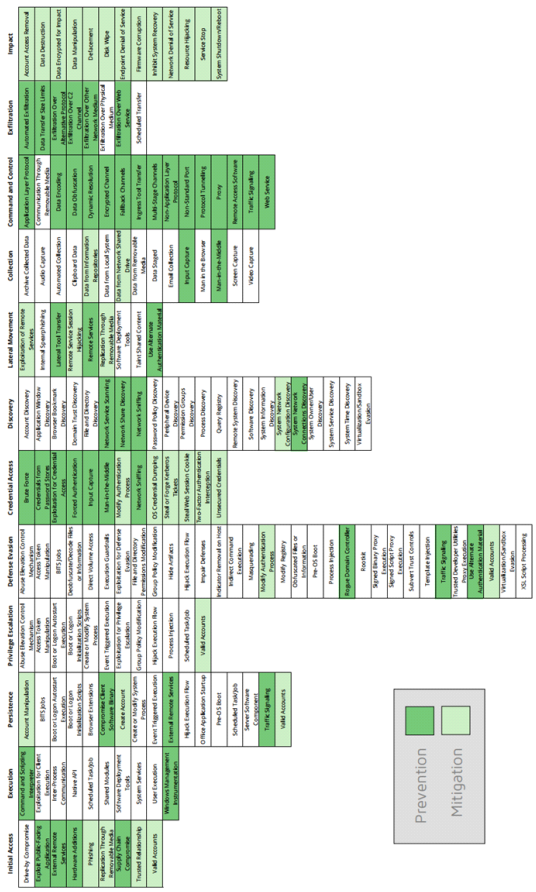
단, 침투시험은 공격TTP를 기반으로 하며 하나의 공격기법(Technique)은 적용대상 환경에 따라 세부적인 구현(Procedure)이 달라질 수 있으므로, 모든 환경에서 동일한 공격TTP를 적용해서 시험을 실시하기에는 한계가 있다. 따라서, 표 3에서는 공격전술(Tactic) 수준으로만 표기하였다.

〔표 3〕 제로트러스트 성숙도 측정을 위한 침투시험(예시)

핵심요소	기능	침투시험용 공격TTP (공격전술)
식별자·신원 (Identity)	식별자 관리	Credential Access Privilege Escalation Collection Discovery
	인증	
	위험도 평가	
	가시성 및 분석	
	자동화 및 통합	
기기 및 엔드포인트 (Device/Endpoint)	정책 준수 모니터링	Initial Access Persistence
	데이터 접근제어	
	자산 관리	
	가시성 및 분석	
	자동화 및 통합	
네트워크 (Network)	네트워크 세분화	Reconnaissance Discovery C2
	위협 대응	
	암호화	
	가시성 및 분석	
	자동화 및 통합	
시스템 (System)	접근통제	Initial Access Persistence Lateral Movement
	시스템 계정 관리	
	네트워크 분리 정책	
	시스템 보안 및 정책 관리	
	가시성 및 분석	
	자동화 및 통합	
응용 및 워크로드 (Application & Workload)	접근 인가	Initial Access Lateral Movement Execution
	위협 보호	
	접근성	
	응용 보안	
	가시성 및 분석	
	자동화 및 통합	
데이터 (Data)	데이터 목록 관리	Exfiltration Impact
	접근 결정방법	
	암호화	
	가시성 및 분석	
	자동화 및 통합	

조직의 환경과 침투시험 역량에 따라 표 3의 예시와 같이 제로트러스트 핵심요소별 침투시험용 공격TTP를 정의할 수 있다. 그러나, 조직마다 핵심요소별 성숙도에 대한 이해와 침투시험 수행능력이 상이하므로, 침투시험용 공격TTP를 가장 합리적으로 선정하는 방법은 해당 핵심요소의 기능을 구현하기 위해 도입하는 기술·솔루션이 어떤 공격TTP를 대응(예방, 완화, 탐지, 차단 등)할 수 있는지를 판단하여 해당 공격TTP를 침투시험에 사용하는 것이다.

그림 6은 특정 제로트러스트 제품이 제시하는 보안효과를 ATT&CK 매트릭스에 매핑한 사례를 보여준다. 이와 같이, 특정 제로트러스트 핵심요소를 구현하는 기술·솔루션의 보안효과를 ATT&CK 매트릭스에 매핑하고 이를 기준으로 침투시험용 공격TTP를 선정하는 것을 고려할 수 있다.



〔그림 6〕 제로트러스트 제품의 보안효과를 ATT&CK 매트릭스에 매핑한 사례[4]

3.2. 제로트러스트 핵심요소별 성숙도 측정

표 3과 같이 정의된 제로트러스트 핵심요소별 침투시험 시나리오를 이용해서 침투시험을 수행하고 그 결과에 따라 핵심요소별 성숙도 수준을 결정한다.

그러나, '식별자 관리' 등과 같이 제로트러스트 솔루션 내부적으로 동작하는 메커니즘은 외부 공격자 관점의 침투시험만으로는 그 동작 여부를 완전하게 확인할 수 없으므로, 일부 기능은 블루팀과 협업(인터뷰, 동작확인 등)하여 성숙도를 확인해야 한다. 이 경우, 레드팀과 블루팀이 실시간으로 협업하는 PTaaS 모델 도입을 고려할 수 있다.

$$S = \{S_1, S_2, S_3, ..., S_n\} \tag{1}$$

$$R(S) = \{Success, Fail\} \tag{2}$$

$$COUNTIF(S, R(S) = Success) \tag{3}$$

수식 1은 표 3에서 정의한 침투시험 시나리오(블루팀 협업 포함)를 의미하며, 수식 2는 특정 침투시험 시나리오에 대한 모의공격의 성공여부를 나타낸다. 수식 3은 전체 침투시험 시나리오에 대해 성공한 개수를 합산한 것을 의미한다.

수식 3에서 나타내는 침투시험 성공개수를 기준으로 제로트러스트 성숙도를 기존, 향상, 최적화의 3단계로 판단할 수 있다. 예를 들어서, 첫 번째 핵심요소인 '식별자·신원'의 경우 전체 5개 기능에 대해서 4~5개 침투시험에 성공하면 성숙도 '기존(Traditional)'으로 판단하고, 2~3개 성공하면 '향상(Advanced)'으로 판단하며, 0~1개 성공하면 '최적화(Optimal)'로 판단할 수 있다. 물론, 세부적인 기준은 조직에서 결정할 수 있으며 이 기준은 일관성을 가져야 한다.

3.3. 제로트러스트 핵심요소별 도입효과 측정

수식 4는 조직이 제로트러스트 도입 전에 측정한 침투시험 성공개수이며, 수식 5는 제로트러스트 도입 후에 측정한 침투시험 성공개수를 의미한다.

따라서, 수식 6과 같이 제로트러스트 도입 전의 침투시험 성공개수와 도입 후의 침투시험 성공개수를 비교하면 제로트러스트 도입효과를 측정할 수 있다. 즉, 제로트러스트 도입으로 인해서 강화되는 보안성의 정도를 측정할 수 있게된다.

$$COUNTIF_{before}(S, R(S) = Success) \tag{4}$$

$$COUNTIF_{after}(S, R(S) = Success) \tag{5}$$

$$\frac{COUNTIF_{before} - COUNTIF_{after}}{COUNTIF_{before}} \tag{6}$$

Ⅳ. 고려사항

이 장에서는 제로트러스트 도입으로 인한 추가적인 보안 고려사항과 제로트러스트의 도입을 촉진하기 위해 수요자 관점에서 요구되는 사항들을 제시한다.

4.1. 제로트러스트 도입에 따른 추가적인 보안위협 검증

제로트러스트의 도입을 통해서 조직의 보안수준을 크게 향상시킬 수 있는 것은 분명한 사실이다[8]. 그러나, 제로트러스트 가이드라인 1.0에서는 제로트러스트 아키텍처의 도입 및 운영으로 인한 추가적인 위협의 발생 가능성을 언급하고 있으며 그에 대한 완화방안을 함께 제시하고 있다[1].

따라서, 제로트러스트 도입·운영 단계에서 발생 가능한 보안위협과 그에 대한 완화조치 적용 여부에 대한 검증이 필요하다.

또한, 제로트러스트 철학을 구축하기 위해 구현된 기술, 솔루션 등에 보안 취약점이 존재할 경우, 제로트러스트 기술·솔루션은 보안을 강화하는 것이 아닌 단일장애지점(Single Point of Failure) 또는 치명적인 사이버 공격의 통로가 될 수 있다는 점에서, 제로트러스트를 구현하는 기술·솔루션에 대한 보안 취약점 검증은 필수적이다.

〔표 4〕 제로트러스트 도입·운영 시 발생 가능한 위협〔1〕

위협	위협완화 방안
제로트러스트 아키텍처 결정 과정 무력화	정책 엔진 및 정책 관리자를 적절하게 설정·모니터링
	모든 설정 변경을 반드시 기록·감사

위협	위협완화 방안
DoS 또는 네트워크 장애	시스템을 적절하게 보호되는 클라우드 환경에서 운영
	사이버 내성에 관한 지침에 따라 여러 위치에 복제
인증 수단 도용 및 내부자 위협	컨텍스트 기반 신뢰도 평가 알고리즘을 통하여, 일반적인 패턴과 다른 리소스 접근 방지
네트워크 가시성	내용을 알 수 없더라도 메타데이터(출발지/목적지 IP 주소 등) 등을 활용하여 공격자 혹은 악성 코드 탐지
	머신러닝 기반 트래픽 분석 등
시스템/네트워크 정보 저장소	중요 기업 데이터는 가장 엄격한 접근제어 정책 설정
전용 데이터 규격 또는 솔루션에 대한 의존	데이터 입력 요소를 도입하기 전, 업체의 보안 통제, 교체 비용, 공급망 위험 관리, 성능, 안전성 등을 종합적으로 고려하여 평가 후 도입
비인간 객체에 의한 제로트러스트 아키텍처 관리	오탐, 미탐에 대해 정기적인 분석 및 수정·보완
	비인간 객체의 접근에 대한 모니터링및 분석

4.2. 위험관리 프레임워크와 연계한 수요자 맞춤형 제로트러스트 도입 및 비용 효율성 증대

제로트러스트 가이드라인 1.0은 국내 기업환경에 대한 공통 보안모델과 도입을 위한 일반적인 방법론을 제시하고 있다. 그러나, 수요자가 자신의 조직의 산업군, 비즈니스 로직, 공격으로 인한 임무영향 등을 기준으로 제로트러스트 성숙도 목표를 설정하고 측정하는데 요구되는 구체적인 방법론은 수요자의 몫으로 남아있다.

국내 민간(ISMS-P), 공공(정보보안관리실태평가), 국방(K-RMF) 등 각 분야별로 많은 조직이 이미 시행중이거나 계획중인 위험관리 프레임워크와 제로트러스트 성숙도 모델을 연계한다면 위험과 그 파급력을 기반으로 비용효율적인 제로트러스트 도입이 가능할 것으로 판단된다.

이를 위한 가칭 '위험관리 기반 성숙도 모델'을 수립하고 이를 운용할 수 있는 세부적인 가이드라인이 제시된다면 제로트러스트 도입의 효과성과 비용 효율성을 획기적으로 증대할 수 있을 것으로 기대한다.

4.3. 제로트러스트 성숙도 측정방법 표준화

제로트러스트로의 전환은 조직의 제로트러스트 핵심요소별 성숙도 목표를 수립하고, 현재 수준 성숙도를 측정한 후, 차이(Gap)를 식별하여 관련 기술·솔루션을 도입하고 목표 성숙도 도달여부를 판단하는 과정이다.

따라서, 제로트러스트 전환을 촉진하기 위해서는 제로트러스트 핵심요소별 성숙도 측정이 매우 중요하며 측정방법에 관한 표준화 논의가 필요하다.

4.4. 자동화 및 통합을 위한 벤더 중립성 보장

제로트러스트 보안모델에서 2가지 교차기능(가시성 및 분석, 자동화 및 통합)은 6가지 모든 핵심요소에 걸쳐 동작해야 한다[1].

그러나, 6가지 핵심요소의 기능에 대해 서로 다른 제조사의 제품을 도입하고, 2가지 교차기능 또한 서로 다른 제조사의 제품을 도입하는 경우, 자동화 및 통합에서 제품간 상호운용성 또는 락인(Lock-in) 이슈가 발생될 가능성이 매우 높다.

따라서, 제로트러스트 보안모델의 각 구성요소(각종 보안 기술·솔루션·서비스)의 연동, 데이터(로그, 탐지규칙, 알람 등) 등에 관한 벤더 중립성 관점의 규격화 및 표준화를 고려하고 이를 가이드라인에 포함할 필요가 있다.

Ⅴ. 결 론

본 연구는 공격자 관점의 침투시험(모의해킹)을 통해서 제로트러스트 핵심요소 6개에 대한 성숙도를 측정하는 방법과, 이를 이용해 제로트러스트 도입 전·후 보안성 강화 효과를 측정하는 방법을 제안하였다.

각 핵심요소 및 기능의 성숙도를 측정하기 위한 침투시험 시나리오의 객관성과 성숙도 측정 접근법은 관련 업계 및 전문가들의 의견을 폭넓게 수렴할 필요가 있다. 또한, 수요자 맞춤형 비용효율적인 제로트러스트 도입을 위해서 위험관리 프레임워크와 연계하는 방법은 추가적인 연구가 필요하며, 자동화 및 통합을 위한 벤더 중립성 보장 방안에 관해서도 산·학·연·관에 걸친 공감대를 형성할 필요가 있다.

향후 공격자 관점의 제로트러스트 성숙도 측정 방법론 고도화 및 위험관리 프레임워크와 연계한 조직

맞춤형 비용효율적 제로트러스트 도입 모델 연구를 통해 국내 제로트러스트 도입·확산에 기여하고자 한다.

참 고 문 헌

[1] “제로트러스트 가이드라인 1.0“, 과기정통부, 한국인터넷진흥원, 한국제로트러스트포럼, June 2023.

[2] “Zero Trust Maturity Model Version 2.0”, CISA(Cybersecurity and Infrastructure Security Agency), April 2023.

[3] ATT&CK for Enterprise v15.1, MITRE Corporation, April 2024.

[4] zentera, “CoIP Access Platform ZTNA and Micro-Segmentation Mapping to the MITRE ATT&CK Matrix for Enterprise”, White Paper, October 2020.

[5] NIST Special Publication 800-207, “Zero Trust Architecture“, NIST, August 2020.

[6] NIST Special Publication 800-37, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy”, NIST, April 2021.

[7] Gartner, “Hyper Cycle for Security Operations”, 2022.

[8] “제로트러스트, 보안 수준 41% 향상시켜”, 데이터넷, December, 2023.

〈저 자 소 개〉

이 철 호 (Cheolho Lee)

종신회원

2002년 2월 : 아주대학교 정보및컴퓨터공학부 졸업

2004년 2월 : 아주대학교 정보통신공학 석사

2010년 3월~현재 : 아주대학교 국방디지털융합학과 박사과정

2004년 2월~현재 : ETRI부설연구소 책임연구원

2022년 12월~현재 : ㈜엔키화이트햇 연구소장

<관심분야> 보안표준, 측정 가능한 보안, 위험관리, 위협정보공유, 제로 트러스트, 레드팀 자동화, BAS

최 창 진 (Changjin Choi)

2013년 2월 : 순천향대학교 정보보호학과 졸업

2016년 2월 : 성균관대학교 정보보호학 석사

2024년 3월~현재 : 가천대학교 정보보호학과 박사과정

2019년 4월~현재 : ㈜엔키화이트햇 이사

<관심분야> BAS, 위협헌팅, 제로 트러스트

정 시 헌 (Siheon Jeong)

2020년 2월 : 영산대학교 사이버보안학과 졸업

2021년 10월~현재 : ㈜엔키화이트햇 컨설팅팀장

<관심분야> 침투시험, 취약점검증

곽 진 (Jin Kwak)

종신회원

성균관대학교 학사, 석사, 박사

전) 정보통신부 통신사무관

전) Special Researcher, Kyushu ISIT, Japan

전) Research Professor. Kyushu University. Japan

현) 국가정보원 암호모듈검증위원회 검증위원

현) 국가정보원 IT보안인증위원회 인증위원

현) 외교부 과학기술외교자문위원회 자문위원

현) 경기남부경찰청 사이버안보자문위원회 자문위원

현) 경기남부경찰철 경찰수사심의위원회 심의위원

현) 국방부 방위산업기술보호실무위원회 자문위원

현) 사이버작전사령부 자문위원

현) Google Cloud Korea Cybersecurity Committee

현) 경기도 교육청 정보화위원회 자문위원

현) 국방부 정책자문위원회 정보화분과 자문위원

국무총리 표창 및 국군방첩사령관 표창 (2023)

문화체육관광부 장관표창 (2022)

과학기술정보통신부 장관표창 (2019)

<관심분야> 암호기술응용, 클라우드보안, 위험관리, 전기차충전보안, 우주사이버보안 등