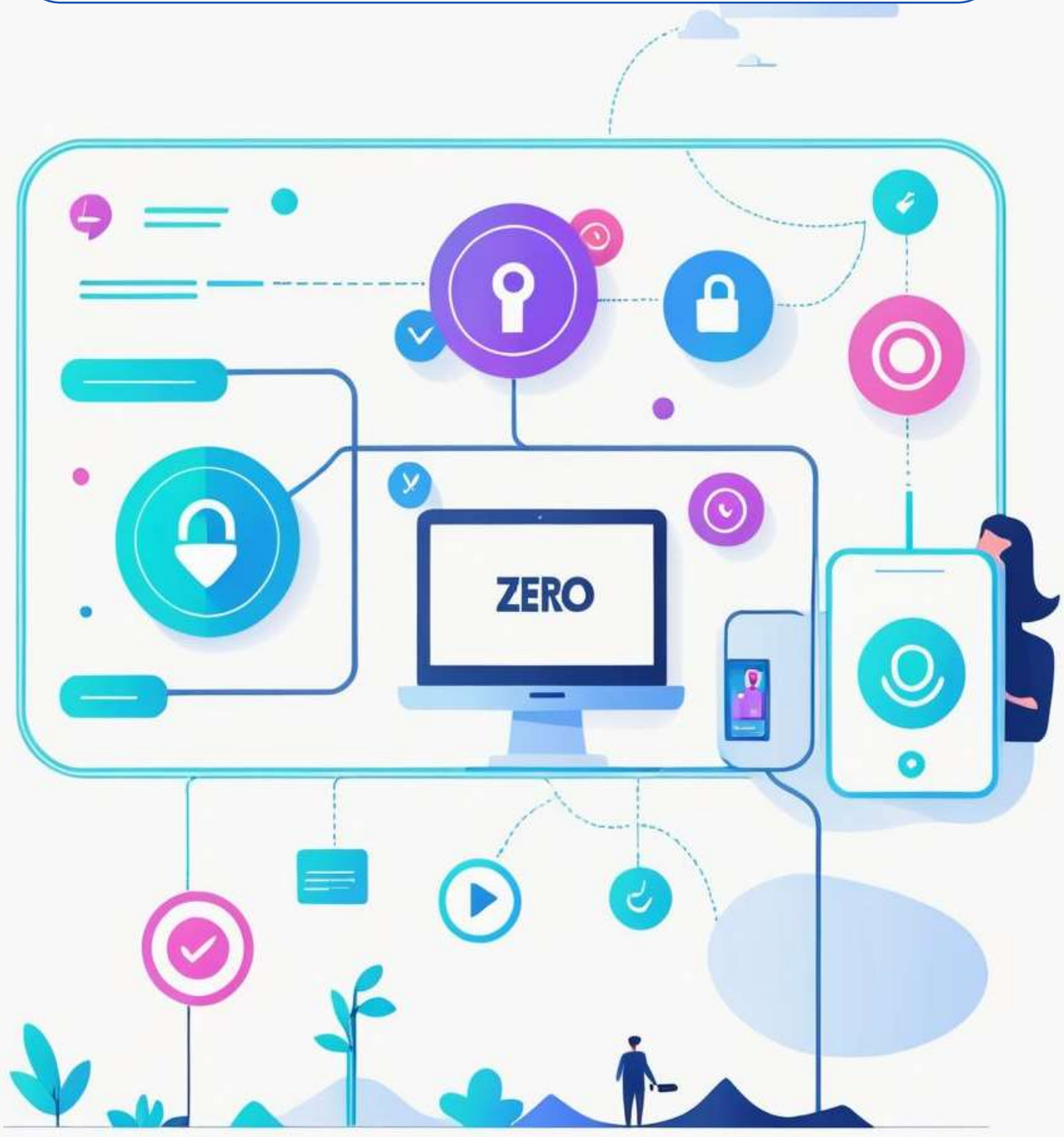
보안 실무자를 위한

제로트러스트 성숙도 모델 해설서



과학기술정보통신부

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목차

제1장 제로트러스트 성숙도 모델 해설서 개요

제2장 제로트러스트 성숙도 모델

제3장 성숙도 수준 평가를 위한 체크리스트 해설

부록

제1장

제로트러스트 성숙도 모델 해설서 개요

1. 성숙도 모델 해설서의 목적 및 구성

2. 성숙도 수준 평가 절차 및 도입 절차

1. 성숙도 모델 해설서의 목적 및 구성

1.1 성숙도 모델 해설서의 목적

현대의 사이버 보안 환경은 전통적인 경계 기반 보안 모델로는 더 이상 효과적으로 대응할 수 없는 복잡하고 다양한 위협들로 가득 차 있으며, 클라우드 컴퓨팅의 확산, 원격 근무의 일반화, IoT 기기의 폭발적 증가, 모바일 기기의 광범위한 활용 등으로 인해 전통적인 네트워크 경계의 개념이 무의미해지고 있는 상황에서 제로트러스트는 이러한 변화에 대응할 수 있는 혁신적인 보안 패러다임으로 주목받고 있다. 그러나 제로트러스트는 단순히 새로운 보안 기술을 도입하는 것이 아니라 조직의 보안 철학과 운영 방식 전반을 근본적으로 변화시키는 것이며, 이러한 변화는 한 번에 이루어질 수 있는 것이 아니라 단계적이고 체계적인 접근을 통해서만 성공적으로 달성할 수 있을 것이다.

제로트러스트 성숙도 모델은 이러한 복잡하고 광범위한 변화 과정을 체계적으로 관리하고 추진할 수 있는 프레임워크를 제공하며, 조직이 현재 어느 단계에 있는지를 객관적으로 평가하고 다음 단계로 나아가기 위해 무엇을 해야 하는지를 명확히 제시함으로써 혼란과 시행착오를 최소화하고 효율적인 구현을 가능하게 한다. 또한, 성숙도 모델은 조직 내 다양한 이해관계자들 간에 공통된 언어와 기준을 제공하여 커뮤니케이션을 원활하게 하고, 경영진의 이해와 지원을 확보하는 데 중요한 역할을 하며, 투자의 우선순위를 결정하고 자원을 효과적으로 배분하는 의사결정 과정에서 객관적인 근거를 제공한다.

본 해설서는 제로트러스트 가이드라인 2.0의 성숙도 수준 평가를 위한 체크리스트에 대한 포괄적이고 실용적인 이해를 제공한다. 먼저 각 항목의 문구와 용어에 대한 명확한 정의와 해석을 제시하여 모호함이나 오해의 소지를 제거하고, 해당 항목이 제로트러스트 전체 아키텍처 내에서 갖는 의미와 역할, 단순한 정의나 설명을 넘어서 해당 항목을 실제로 구현하는 기반 기술에 대한 설명과 성숙도 수준을 증명할 수 있는 증적 자료를 제시하고 있다. 본 해설서는 다음과 같은 구조화된 해설을 제공한다.

첫째, 체크리스트 항목의 핵심 목적과 달성하고자 하는 보안 목표를 명확히 정의한다.

둘째, 성숙도 레벨별로 요구되는 구현 수준과 평가 기준을 구체적으로 제시한다.

셋째, 다양한 조직 환경과 규모에 맞는 실제 성숙도 수준 평가 시 기술적 사례를 제공한다.

본 해설서는 제로트러스트 성숙도 분석 방법론에 기반하여 6대 핵심 요소와 교차 기능에 대한 각 세부역량 및 문항에 대한 분석 방안을 제시함으로써 조직이 제로트러스트 아키텍처 구현 현황을 체계적으로 평가할 수 있도록 상세한 가이드를 제공한다.

1.2 성숙도 모델 해설서 구성

상기 목적을 위하여 본 해설서는 다음과 같이 구성하였다.

제1장에서는 해설서 개발의 목적과 구성에 대해서 살펴보고, 성숙도 수준 평가 절차와 평가 기반 제로트러스트를 도입하는 절차를 기술하였다.

- 성숙도 모델 해설서의 목적 및 구성
- 성숙도 수준 평가 절차 및 평가 기반 제로트러스트 도입 절차

제2장에서는 제로트러스트 성숙도 모델의 성숙도 수준에 대한 정의와 성숙도 모델의 구조에 대해서 설명하고 있다. 제로트러스트 도입을 위해 반드시 고려해야 할 성숙도 수준 평가의 의미와 활용 방안에 대해 소개한 후, 구체적인 성숙도 모델의 구조에 대해서 설명하고 있다.

- 성숙도 모델 소개
- 성숙도 모델 구조에 대한 설명
- 성숙도 수준에 대한 설명

제3장에서는 제로트러스트 가이드라인의 각 핵심 요소별 세부 역량에 대한 성숙도 수준 평가를 위한 체크리스트에 대한 상세한 설명을 다루고 있다. 이 장에서는 실무진이 즉시 활용할 수 있는 구체적이고 실용적인 내용을 제공하고 있으며 각 체크리스트 항목에 대해 '무엇을', '어떻게', '왜' 구현해야 하는지를 명확히 제시하고자 하며 각 체크리스트 항목에 대해 다음과 같은 구조화된 해설을 제공하고 있다.

- 가이드라인 2.0의 성숙도 수준 평가를 위한 체크리스트 각 항목에 대한 명확하고 상세한 해석 제공
- 각 체크리스트 항목에 대한 구체적인 구현 방법과 기술적 솔루션 안내
- 복잡한 기술 용어와 개념을 실무진이 쉽게 이해할 수 있도록 구체적 사례와 함께 설명

이 외에 **부록**에서는 각 성숙도 수준에서 요구하는 기능에 대한 기술 도입을 고려한 보안 세부 역량 및 이를 뒷받침 할 수 있는 솔루션 및 증적 자료 예시를 안내하고 있으며, 본 해설서의 이해를 돕기 위하여 용어 및 약어 정리를 수록하였다.

[표 1] 이해관계자별 참고 권장 부분

역할	참고 권장 부분
경영진 및 관리자	제1장 제로트러스트 성숙도 모델 해설서 개요 ····· P.6 제2장 제로트러스트 성숙도 모델 ····· P.16
정보보안 담당자 및 시스템 관리자	제3장 성숙도 수준 평가를 위한 체크리스트 해설 ····· P.42

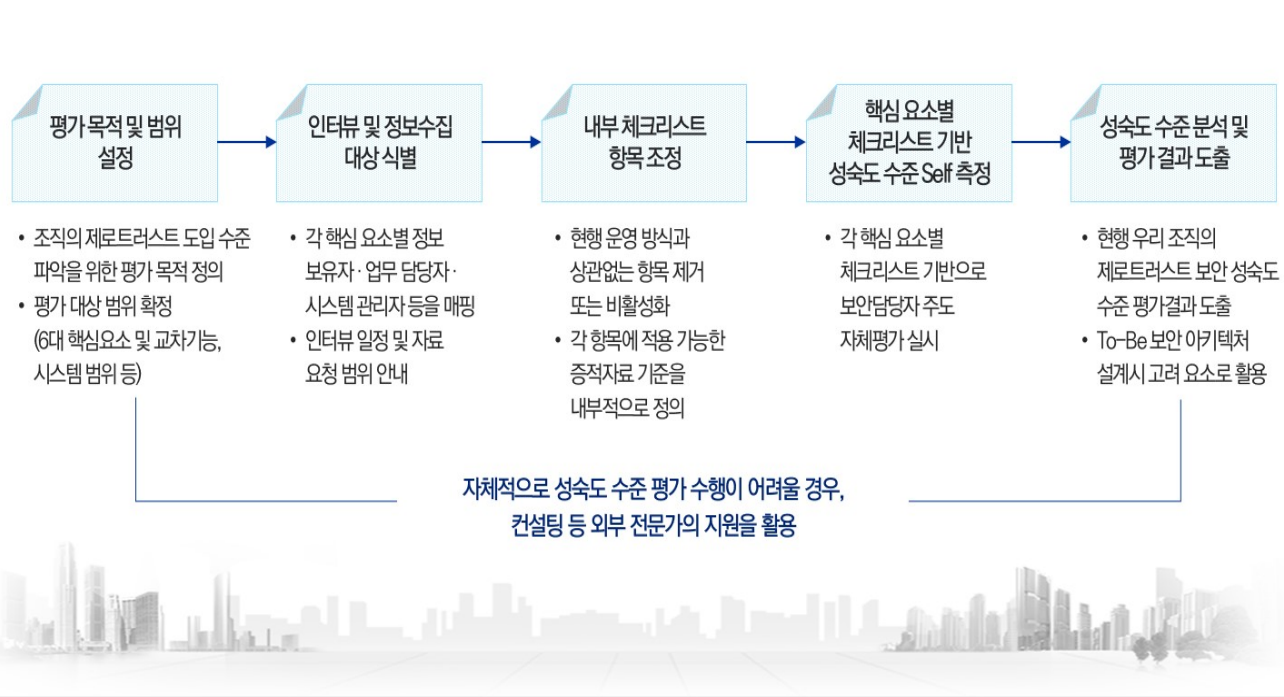
2. 성숙도 수준 평가 절차 및 도입 절차

기업의 보안 환경은 규모, 적용 규제, 보안 투자 수준, 보유 중인 보안 장비와 서비스 구성 등 다양한 요소에 따라 상이하게 형성된다. 일부 조직은 기존의 망분리 규제를 지속적으로 적용해야 하지만, 다른 조직은 망분리 제약 없이 클라우드 서비스를 적극적으로 활용하고 있는 등 운영 환경에도 큰 차이가 존재한다. 이와 같이 조직별로 상이한 여건과 보안 운영 방식에 따라 제로트러스트 성숙도 수준 평가는 각 환경의 특성을 충분히 고려하여 수행될 필요가 있다. 가이드라인 2.0의 성숙도 수준 평가 체크리스트는 이러한 다양한 상황과 관점에 비추어 제로트러스트 보안 규제를 일률적 보안 규제로 정의하지 않고, 제로트러스트 도입 전략 수립 과정에서 반드시 검토해야 할 사항을 강조함으로써 도입 전략 수립을 지원하고 도입 후 보안 수준 및 효과성 분석 방안 제시를 통해 보안 모델을 어떻게 지속적으로 개선해 나갈 수 있을지에 대한 방향성 설정에 도움을 주고 있다. 따라서, 본 성숙도 수준 평가 절차는 기업이 스스로 가이드라인 2.0을 기반으로 현행 수준을 점검하고, 향후 제로트러스트 구현 전략을 수립하는 데 유용한 기준이 될 것이다.

2.1 성숙도 수준 평가 절차

성숙도 수준 평가는 **① 평가 목적 및 범위 설정, ② 인터뷰 및 정보수집 대상 식별, ③ 내부 체크리스트 항목 조정, ④ 성숙도 수준 평가 수행, ⑤ 성숙도 분석 및 평가 결과 도출**의 5단계 절차로 이루어진다.

[그림 1] 제로트러스트 성숙도 수준 평가 절차



먼저 제로트러스트 성숙도 수준 평가의 첫 단계는 조직이 평가를 수행하는 목적과 기대하는 결과를 명확히 정의하는 것이다. 보안 담당자는 조직의 업무 특성, 보호해야 할 자산, 적용받는 규제 요건 등을 검토하여 평가가 다루어야 할 범위를 설정한다. 이 과정에서 조직의 네트워크 구조, 시스템 구성, 보안 정책 체계와 같은 기반 정보를 함께 정리함으로써 이후 평가 과정에서의 이해도를 높인다.

두 번째로, 성숙도 수준 평가를 위한 인터뷰 및 정보수집 대상자를 식별해야 한다. 조직 내 각 보안 영역을 담당하는 전문가가 누구인지 파악하는 것은 정확한 성숙도 수준 평가를 위한 필수 과정이다. 보안 담당자는 통합계정권한 담당자, 네트워크 관리자, 서버 운영팀, 데이터 관리 부서 등 각 핵심 요소별 정보 보유자를 식별하고 인터뷰 일정을 조율한다. 동시에 필요한 로그, 정책 문서, 절차서 등 사전 정보수집 항목도 함께 정리하여 평가의 준비도를 높인다.

세 번째로, 체크리스트 항목 조정은 제로트러스트 가이드라인 2.0에서 제공하고 있는 성숙도 수준 평가를 위한 체크리스트를 **각 기업의 IT 환경에 적합한 형태로 조정**하는 과정이다. 모든 조직이 동일하게 적용할 수 있는 일률적인 기준이 아니기 때문에, 보안 담당자는 자사 상황에 맞지 않는 항목을 비활성화하거나 수정할 수 있다. 아래 그림은 시스템 핵심 요소 중 시스템 환경에 따른 정책 관리 역량에 대한 체크리스트 문항으로 클라우드에 대한 내용을 다루지만, 실제 기업이 향후에 클라우드 도입 등을 계획하고 있다면 미리 점검하는 등의 취지로 체크리스트를 활용할 수 있다.

[그림 2] 제로트러스트 가이드라인 2.0 성숙도 수준 평가 체크리스트 – 시스템 환경에 따른 정책 관리

세부역량	확인방법	성숙도	Check
시스템 환경에 따른 정책 관리	• 온프레미스 환경에서 보안 정책을 수립하고 있는가?	기존	☐
	• 수동으로 보안 정책을 유지·관리하고 있는가?	기존	☐
	• 클라우드 환경으로 전환하면서 보안 정책을 각각에 맞게 수립하고 있는가?	초기	☐
	• 정책이 자동으로 적용되는가?	초기	☐
	• 하이브리드 클라우드 환경으로 전환되면서 실시간으로 보안정책이 조정되는가?	향상	☐
	• 환경 변화에 따라 정책이 동적으로 변경 가능한가?	향상	☐
	• 보안 위협에 맞춘 자율적인 정책 적용이 가능한가?	최적화	☐
	• 정책 관리가 완전히 자동화되어, 변화하는 환경에서도 일관된 보안 정책을 유지할 수 있는가?	최적화	☐

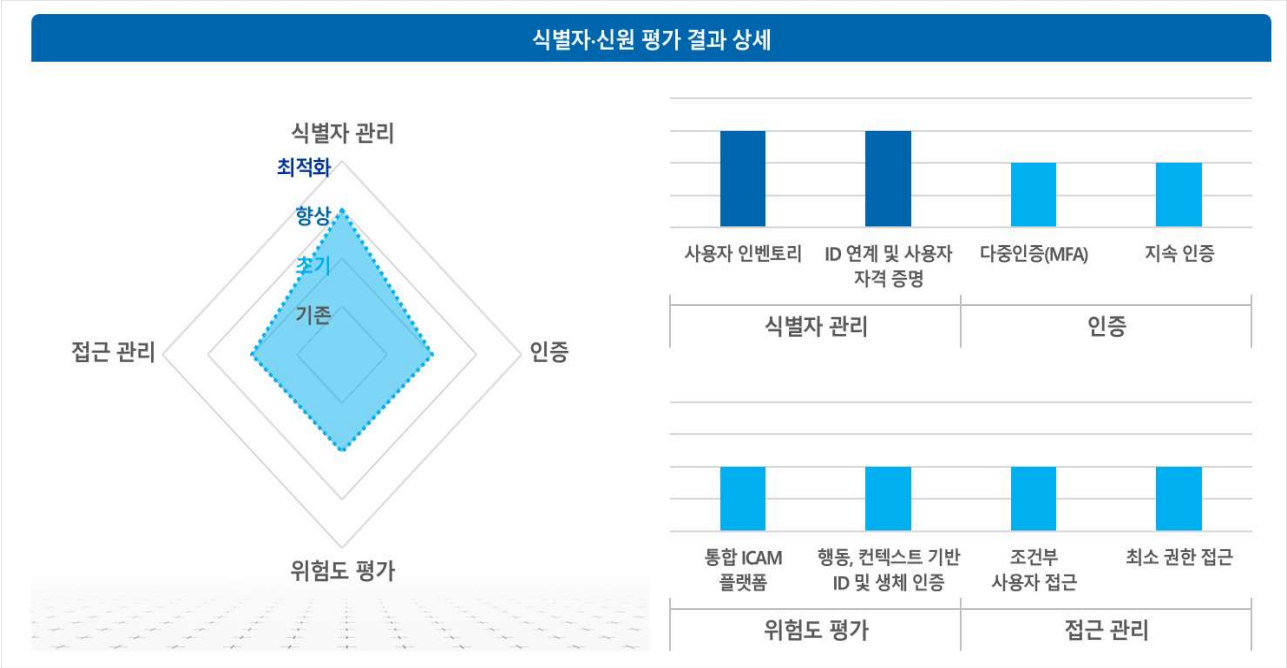
출처: KISA, 제로트러스트 가이드라인 2.0

네 번째로, 성숙도 수준 평가 수행은 조정된 체크리스트를 기반으로 조직의 현행 수준을 사실에 기반해 스스로 평가한다. 조직의 업무 수행 상황에 따라 한 명의 담당자가 여러 영역을 혹은 다수의 담당자가 하나의 영역에 대해 평가를 진행하기도 한다.

마지막으로 성숙도 수준 평가 결과를 도출하게 된다. 성숙도 결과는 현재 기업의 제로트러스트 성숙도 수준을 나타내는 **현재 수준**과 향후 기업이 도달해야 할 **목표 수준**을 보여준다. 현재 수준은 기업이 제로트러스트를 구성하는 각 요소의 영역별로 현재 어느 단계까지 이행하고 있는지 평가한 결과이며, 목표 수준은 현재의 성숙도 수준을 바탕으로 기업의 목표와 보안 환경을 고려하여 도달하고자 하는 수준을 설정한 것이다.

아래의 상세 결과 예시는 체크리스트 기반 성숙도 수준 평가 방식을 활용하여 도출한 기업의 기능별 현재 수준을 시각화한 것이다. 해당 방식에서는 각 단계별 체크리스트 항목을 **모두 충족해야 해당 수준을 달성**한 것으로 보고 있으며, **상위 단계의 항목을 달성하기 위해서는 하위 단계 항목들이 선행**되어야 한다는 기준을 정의하였다.

[그림 3] 제로트러스트 성숙도 수준 평가 상세 결과 예시



이러한 정의를 통해 기업은 현재 수준을 명확히 파악하고, 기능별 격차에 따라 도출된 개선 과제를 우선순위에 따라 체계적으로 추진할 수 있다. 만약, 조직의 내부 역량만으로 평가가 어려운 경우에는 컨설팅 등 외부 전문가의 지원 활용을 고려할 수 있다.

2.2 성숙도 수준 평가 기반 도입 절차

앞서 진행한 성숙도 수준 평가 결과를 기반으로 기업은 실제 **제로트러스트 적용을 위한 일련의 프로세스를 수행**할 수 있다. 설정한 목표 수준을 실제 조직의 환경을 고려하여 조정, 해당 목표 달성을 위한 과제를 도출, 과제 이행을 위한 로드맵을 수립하고 이행함으로써 제로트러스트 단계별 적용이 가능해진다. 이러한 과정의 상세 내용은 아래와 같다.

[그림 4] 제로트러스트 성숙도 수준 평가 기반 도입 절차

① 목표 수준 정의

성숙도 수준 평가를 통해 정의한 **초기 목표 수준을 조직의 현실적인 조건과 실행 가능성을 반영하여 조정**한다. 예산, 인력, 기술, 비즈니스 환경 등을 종합적으로 고려하여 실질적으로 달성 가능한 목표를 정의한다. 모든 조직이 최고 수준의 성숙도를 목표로 할 필요는 없으며, 자신의 환경과 상황에 적합한 현실적이고 달성 가능한 목표를 수립하는 것이 중요하다. 예를 들어, 금융기관이나 의료기관처럼 높은 수준의 보안이 요구되는 조직은 고도화된 성숙도를 목표로 설정할 수 있지만, 상대적으로 보안 위협이 낮은 조직은 중간 수준의 성숙도를 단계적 목표로 설정할 수 있다. 목표 수준 설정 시에는 단기 목표와 장기 목표를 구분하여 수립하는 것이 좋다. 일반적으로 1년 이내의 단기 목표는 기본적인 제로트러스트 원칙을 적용하고 핵심 취약점을 해소하는 데 집중하며, 3년에서 5년의 장기 목표는 조직 전체에 제로트러스트를 완전히 내재화하고 지속적인 개선 체계를 구축하는 수준으로 설정한다. 이러한 단계별 목표 설정은 조직 구성원들에게 명확한 방향성을 제시하고, 점진적인 성과 달성을 통해 변화에 대한 동기부여를 제공한다. 만약 특정 목표 수준을 정의하기 어렵다면 각 역량별 현재 수준을 다음 단계로 끌어올리는 목표를 선정하는 방법을 권장한다.

② Gap 분석 및 개선 과제 도출

기업의 제로트러스트 현재 수준과 목표 수준 간 Gap 분석은 조직이 제로트러스트 보안 체계를 효과적으로 구축하고 발전시키기 위한 출발점이자 전략 수립의 핵심 기반이 된다. 이 분석을 통해 조직은 현재 보유한 보안 역량과 도달하고자 하는 목표 간의 격차를 객관적으로 파악하고, 이를 해소하기 위한 구체적이고 실행 가능한 로드맵을 수립할 수 있다. 각 평가 영역별로 현재 수준과 목표 수준을 비교하고, 격차가 큰 영역을 우선순위로 식별한다. 단순히 점수 차이만 보는 것이 아니라, 격차의 근본 원인 파악이 필요하다. 기술 부족인지, 정책 미비인지, 프로세스 부재인지, 예산 제약인지, 인력 역량 부족인지 등을 명확히 분석하여 각 격차에 대한 해소 방안을 구체화한다. 또한, Gap 분석에서는 영역 간 상호 의존성과 우선순위를 면밀히 고려해야 한다. 제로트러스트의 각 구성요소는 독립적으로 작동하는 것이 아니라 유기적으로 연결되어 있으므로, 특정 영역의 격차가 다른 영역의 구현을 제약할 수도 있기 때문이다. 예를 들어,

신원 관리 체계가 미흡하면 접근제어와 모니터링의 효과성이 떨어지며, 네트워크 가시성이 확보되지 않으면 위협 탐지와 대응이 어려워진다. 따라서 **기반이 되는 핵심 영역을 우선적으로 개선**하고, 이를 기반으로 **다른 영역을 점진적으로 강화**하는 전략적 접근이 필요하다.

③ 보안 모델 설계

도출된 개선 과제를 기반으로 현행 정보보안 아키텍처에 PDP, PEP, PIP 등 제로트러스트 관점의 To-Be 보안 모델을 설계한다. 모델 설계 시 **1) 인증체계 강화, 2) 마이크로 세그멘테이션, 3) 소프트웨어 정의 경계** 등 제로트러스트 구현의 3가지 원칙을 준수하여 설계한다.

첫째, 인증체계 강화 측면에서는 신원을 새로운 보안 경계로 설정하고 모든 접근 요청 시 사용자·디바이스·환경 정보를 기반으로 한 다중 요소 인증과 지속적 검증을 수행한다. 사용자 계정뿐만 아니라 디바이스 보안상태, 위치 정보, 접속 시간, 행동 패턴 등 다양한 컨텍스트를 종합하여 위험 수준을 평가하고, 이에 따라 적응형 인증 및 동적 접근제어를 적용한다.

둘째, 마이크로 세그멘테이션을 통해 네트워크를 논리적으로 세분화하고 각 세그먼트를 독립적인 보호 영역으로 구성하여, 전통적인 네트워크 경계 방어와 달리, 제로트러스트에서는 네트워크 내부를 더 이상 신뢰 영역으로 간주하지 않으므로, 애플리케이션, 워크로드, 사용자 그룹별로 세밀한 세그먼트를 구성하여 횡적 이동을 차단한다. 각 세그먼트 간 통신은 명시적으로 정의된 정책에 의해서만 허용되며, 불필요한 네트워크 경로는 원칙적으로 차단하는 모델을 설계한다.

셋째, 소프트웨어 정의 경계 원칙을 기반으로 검증된 사용자와 검증된 디바이스에게만 최소한의 네트워크 가시성과 접근권한을 부여한다. 소프트웨어 정의 경계는 사용자 요청마다 동적으로 세션을 생성하고 허용된 리소스만 노출함으로써, 기존 경계 기반 모델에서 발생하던 과도한 네트워크 노출을 근본적으로 최소화한다.

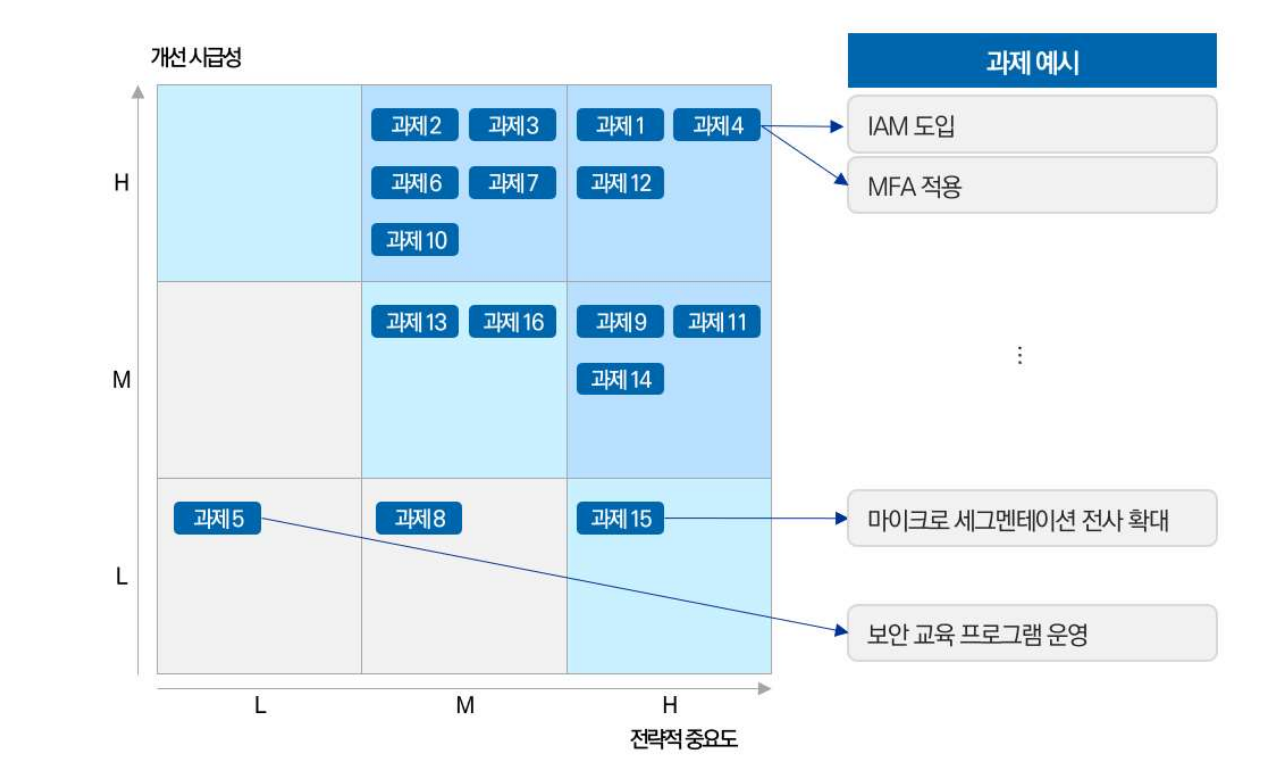
최소 권한 원칙 적용은 사용자와 애플리케이션에 대해 업무 수행에 필요한 최소한의 권한만 부여하며, 시간 제한, 세션 제한, 범위 제한 등을 통해 권한의 남용이나 오용을 방지해야 한다. 권한 부여는 정적이 아닌 동적으로 이루어져야 하며, 접근 요청 시마다 현재의 컨텍스트와 위험 수준을 재평가하여 실시간으로 권한을 조정 할 수 있어야 한다.

이러한 보안 영역을 지속적으로 모니터링하고 가시성을 확보할 수 있어야 한다. 제로트러스트 환경에서는 모든 사용자 활동, 디바이스 상태, 네트워크 트래픽, 애플리케이션 동작을 실시간으로 모니터링하고 로그를 수집해야 한다. 수집된 데이터는 보안 정보 및 이벤트 관리 시스템, 사용자 및 개체 행동 분석 도구, 위협 인텔리전스 플랫폼 등을 통해 분석되며, 비정상 행위나 위협 징후를 조기에 탐지하여 자동화된 대응을 수행할 수 있어야 한다.

④ 로드맵 수립

도출된 과제를 기반으로 **제로트러스트 단계적 도입을 위한 로드맵을 수립**하는 단계로, 먼저 앞서 도출된 과제의 **전략적 중요도**와 **개선 시급성**을 기준으로 이행 우선순위를 설정한다. 전략적 중요도는 해당 과제가 대고객 접점 업무 또는 핵심 업무와 직결되는지, 그리고 향후 손익 개선이나 비용 절감에 기여할 수 있는지를 기준으로 판단한다. 개선 시급성은 시장·경쟁사 동향과 법·제도 변화 등을 고려하여 단기간 내 이행이 필요한 과제인지 여부를 기준으로 판단한다. 일반적으로 높은 보안 위험을 해소하면서 상대적으로 구현이 용이한 항목을 우선 추진하여 빠른 성과를 만들어내고, 이를 기반으로 복잡하고 장기적인 개선 과제를 단계적으로 진행하는 접근이 효과적이다. 또한 경영진의 지원을 확보하고 조직 전체의 관심을 환기시키기 위해, 가시적인 성과를 낼 수 있는 퀵윈(Quick-Win) 프로젝트를 초기에 포함하는 것도 중요하다. 다음은 우선순위 선정을 위한 전략적 중요도와 개선 시급성에 대한 사항이다.

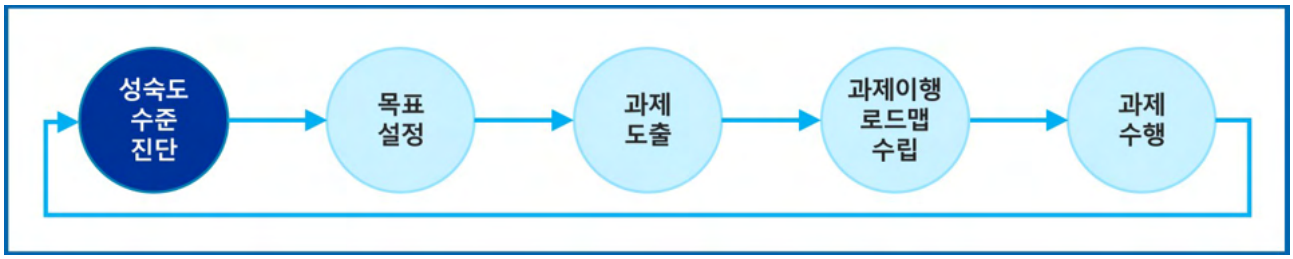
[그림 5] 전략적 중요도와 개선 시급성에 따른 우선순위 설정



마지막으로 이행 우선순위에 따른 실행 연도, 기업의 내외부 환경, 투자계획 등을 고려한 중장기 로드맵을 수립한다.

제로트러스트 도입을 위한 컨설팅 결과물은 경영진과 주요 이해관계자에게 효과적으로 전달해야 한다. 기술적인 세부사항보다는 비즈니스 관점에서 현재 보안 위험 수준, 격차 해소의 필요성, 예상되는 투자 대비 효과, 구현 일정 등을 명확하게 설명해야 한다. 시각화된 대시보드, 성숙도 레이더 차트, 로드맵 타임라인 등을 활용하여 복잡한 정보를 직관적으로 전달하고, 의사결정에 필요한 핵심 정보를 제공해야 한다.

[그림 6] 제로트러스트 도입·전환 프레임워크



제로트러스트는 단순히 특정 기술이나 제품을 도입하는 것이 아니라, 조직의 전반적인 보안 철학과 접근 방식을 근본적으로 재정립하는 전략적 여정이다. 로드맵 이행 이후에는 새롭게 현재의 성숙도 수준을 평가하고 목표를 재설정한 후 새로운 과제 수행을 위한 로드맵을 수립하는 등 일회성이 아니라 **지속적으로 점검하고 반복하는 과정을 통해 기업의 제로트러스트 수준을 향상**시켜야 한다. 일반적으로 분기별 또는 반기별로 성숙도를 재평가하고, 연간 단위로 목표와 전략을 재수립하는 사이클을 운영하는 것이 바람직하다. 이러한 지속적인 평가와 개선을 통해 조직은 제로트러스트 성숙도를 점진적으로 향상시키고, 변화하는 보안 환경에 효과적으로 대응할 수 있는 역량을 확보할 수 있다.

제2장

제로트러스트 성숙도 모델

1. 성숙도 모델 소개
2. 성숙도 모델 구조
3. 성숙도 수준 평가 요소
4. 성숙도 수준 정의

1. 성숙도 모델 소개

1.1 성숙도 모델의 개념

성숙도 수준 평가는 조직의 특정 프로세스, 기술, 또는 역량이 얼마나 체계적이고 효과적으로 구성되어 있는지를 단계별로 측정하고 평가하는 체계적인 방법론이다. 성숙도 수준 평가의 핵심 개념은 조직의 역량을 여러 개선 단계로 구분하여 각 단계마다 특정한 특징과 요구사항을 정의하는 것이다. 일반적으로 낮은 단계에서는 비공식적이고 임시방편적인 프로세스가 주를 이루며, 단계가 높아질수록 표준화되고 문서화된 프로세스, 측정 가능한 지표, 지속적인 개선 체계 등이 자리 잡게 된다. 각 단계에서는 이전 단계의 역량을 기반으로 하며, 단계적으로 발전해 나가는 로드맵을 제시하는 것이다.

KISA 제로트러스트 가이드라인 2.0의 성숙도 모델은 조직의 제로트러스트 보안 수준을 체계적으로 평가하고 개선할 수 있는 포괄적인 프레임워크이다. 성숙도 모델은 단순히 기술적 완성도를 측정하는 도구를 넘어서, 조직이 현재 어디에 위치하고 있으며 어디로 나아가야 하는지를 명확히 보여주는 전략적 나침반 역할을 수행한다. 가이드라인 2.0의 성숙도 모델의 기본 구조는 4단계로 구성되어 있으며, 이는 가이드라인 1.0의 3단계 모델에서 '초기' 단계를 추가하여 더욱 세분화하였다.

1.2 성숙도 모델의 활용 가치

제로트러스트 도입은 단기간에 실현되기 어려운 복잡하고 장기적인 과제이다. 제로트러스트 성숙도 모델은 기존 경계 기반 보안에서 제로트러스트 아키텍처로 전환하려는 조직이 **효율적인 자원 투자를 통한 단계적 전략을 설정**할 수 있도록 도움을 준다는 점에서 아래와 같은 의의를 가진다.

첫째, 제로트러스트 성숙도 모델은 기존의 ROI(투자 대비 수익률) 중심 접근만으로는 파악하기 어려웠던 보안 관리 수준을 체계적으로 진단할 수 있는 근거를 제공한다. 많은 조직이 보안 수준을 주관적 판단이나 일부 지표에만 의존하는 경우가 많은데, 성숙도 수준 평가는 신원 관리, 디바이스 보안, 네트워크 환경, 애플리케이션 보호, 데이터 보안, 가시성 및 분석 등 제로트러스트의 핵심 요소 전반을 포괄적으로 검토함으로써 조직의 보안 역량을 보다 명확하게 파악할 수 있다. 이를 통해 보안 담당자는 막연하게 느끼던 취약 영역을 구체적으로 식별하고, 상대적으로 강점이 있는 영역과 개선이 필요한 영역을 구조적으로 구분할 수 있다. 이러한 분석 결과는 향후 보안 투자 방향을 합리적으로 판단하고, 필요한 기술·인력·프로세스 측면의 개선 우선순위를 설정하는 데 중요한 참고자료가 된다.

둘째, 기존 경계 기반 보안에서 제로트러스트 아키텍처로 전환하려는 조직에게 **명확한 로드맵을 제시**한다. 성숙도 모델을 바탕으로 조직의 현재 성숙도 수준을 측정하고, 향후 수행해야 할 보안 과제와 우선순위를 식별할 수 있다. 제로트러스트로의 전환은 하루아침에 이루어질 수 없으며

조직의 규모, 업종, 보유자원, 규제 요구사항 등에 따라 목표로 하는 성숙도 수준이 다를 수 있다. 성숙도 수준 평가는 조직이 달성해야 할 현실적이고 적절한 목표 수준을 설정하고, 현재 상태와의 격차를 세부 영역별로 분석하여 어떤 부분을 먼저 개선해야 하는지, 어떤 순서로 투자를 집행해야 하는지에 대한 명확한 근거를 제시한다. 이는 한정된 예산과 인력을 가장 효과적으로 배분하여 보안 투자 대비 효과를 극대화하는 데 필수적이다.

셋째, 경영진과 의사결정권자를 설득하고 조직 전체의 공감대를 형성하는 강력한 커뮤니케이션 도구로써의 역할이다. 보안 담당자가 추상적으로 "제로트러스트가 필요합니다"라고 말하는 것과, 성숙도 수준 평가 결과를 바탕으로 "우리 조직은 현재 기존 단계에 있으며, 초기 단계로 발전하기 위해서는 다단계인증 도입과, 마이크로 세그멘테이션 구현, 실시간 모니터링 강화가 필요하고, 이를 위해 n억원의 투자가 필요합니다" 라고 구체적으로 제시하는 것은 설득력에서 큰 차이가 있다. 특히 성숙도 수준 평가 결과를 시각화된 대시보드나 레이더 차트로 표현하면, 기술적 배경이 없는 경영진도 현재 상황과 개선 방향을 직관적으로 이해할 수 있어 의사결정 과정이 신속해진다.

넷째, 제로트러스트 도입 프로젝트의 진행 상황을 추적하고 성과를 측정하는 명확한 기준을 제공한다. 제로트러스트 전환은 수개월에서 수년에 걸친 장기 프로젝트이므로, 중간단계에서 "우리가 올바른 방향으로 가고 있는가"를 확인할 수 있는 측정 도구가 필요하다. 정기적인 성숙도 재평가를 통해 각 영역별로 어느 정도 개선이 이루어졌는지를 정량적으로 확인할 수 있으며, 이는 프로젝트팀의 사기를 높이고 지속적인 추진 동력을 제공하며 예상보다 진척이 느린 영역을 조기에 발견하여 문제를 해결하거나 계획을 조정할 수 있는 기회를 제공한다.

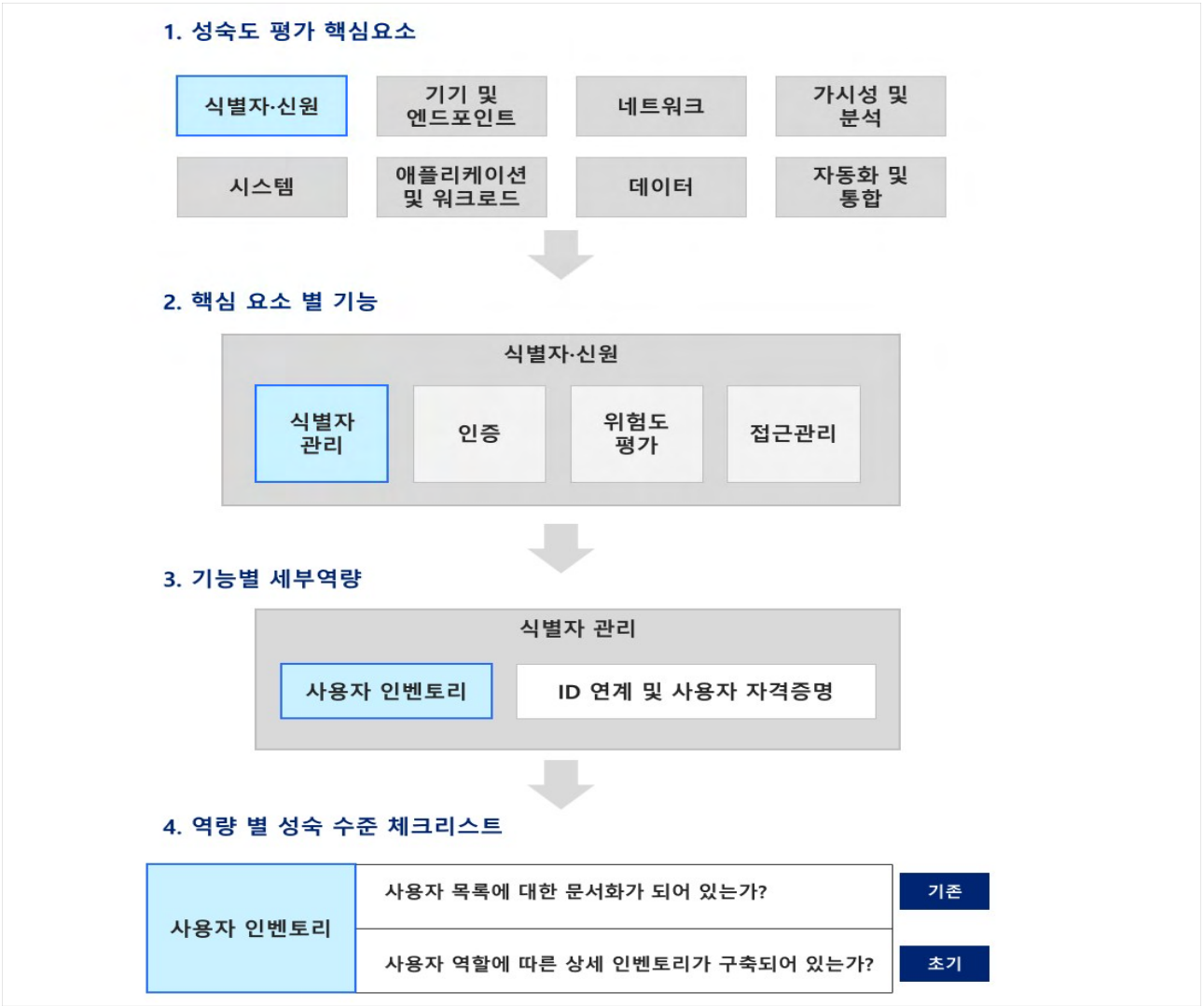
다섯째, 조직 내 보안 문화를 개선하고 지속적인 개선 마인드를 정착시킨다는 점이다. 성숙도 수준 평가는 보안이 한번 구축하면 끝나는 것이 아니라 지속적으로 평가하고 개선해야 하는 순환적 프로세스임을 조직 구성원들에게 각인시키며 정기적인 평가와 개선 활동을 통해 보안 담당자뿐만 아니라 일반 직원들도 제로트러스트 원칙과 보안의 중요성을 이해하게 되며, 이는 조직 전체의 보안 의식 수준을 높이는 효과를 가져온다. 보안이 IT 부서만의 책임이 아니라 모든 구성원이 참여해야 하는 전사적 과제라는 인식 확산에 도움을 줄 수 있다.

마지막으로, 제로트러스트 성숙도 모델은 규제 준수와 인증 준비에 체계적으로 활용될 수 있다. ISMS-P, ISO 27001 등 주요 인증과 금융·의료·통신 등 산업별 규제 요구사항은 제로트러스트의 핵심 원칙과 여러 측면에서 연관성을 갖는다. 성숙도 수준 평가를 통해 조직의 보안 관리체계를 정비하고 운영 절차를 명확히 하는 과정은 규제 준수 준비도를 높이는 데 도움을 주며, 관련 활동을 보다 구조적이고 일관되게 수행할 수 있게 한다. 또한 평가 과정에서 정리되는 정책, 절차, 증적 자료 등은 규제 기관이나 감사 기관이 요구하는 문서화를 지원하는 기반 자료로 활용될 수 있다.

2. 성숙도 모델 구조

제로트러스트 성숙도 모델은 크게 6가지 핵심 요소(식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 애플리케이션 및 워크로드, 데이터)와 2가지 교차 기능(가시성 및 분석, 자동화 및 통합)으로 나뉘어지며, **각 요소를 구성하는 기능과 이를 구현하기 위한 세부역량으로 구성**되어 있다. 기존의 성숙도 모델은 단계별 권고사항이 추상적이고 일반적인 수준에 그쳐, 실제 보안 담당자가 기술과 정책을 구체적으로 도입하는 데 어려움을 겪는 한계가 있었다. 이를 보완하기 위해 제로트러스트 가이드라인 2.0에서는 제로트러스트 적용을 위한 실질적인 기준을 제공하고 보안 실무자가 각 단계에서 수행해야 할 조치를 명확히 파악할 수 있도록 각 기능을 구성하는 세부역량을 정의하였다.

[그림 7] 제로트러스트 성숙도 모델 구조



2.1 핵심 요소

제로트러스트 성숙도 모델의 **6가지 핵심 요소와 2가지 교차 기능**은 제로트러스트 관점에서 기업망의 보안성을 개선하기 위하여 무엇을 보호해야 하는가에 대한 답으로 볼 수 있다. 조금 더 살펴보면, 기업망에서 가장 중요한 보호의 대상은 데이터(Data)로 볼 수 있다. 식별자(Identity)로 구분되는 사용자는 기기(Device)를 이용하여 기업 네트워크(Network)상에서 애플리케이션 및 워크로드(Application & Workload)를 통해 데이터에 접근하게 되며, 데이터는 중요 데이터 서버 등 시스템(System)에 위치할 수 있다. 이들은 모두 사이버 공격 대상이 될 수 있어, 제로트러스트 관점에서 기업망의 핵심 요소로 볼 수 있다.

① 식별자·신원(Identity): "누가 접근하는가?"에 대한 신뢰 검증 영역으로, 사용자는 물론 서비스 계정, 시스템 계정까지 모든 주체를 명확히 식별하고, 지속적으로 인증·인가하는 체계이다.

② 기기 및 엔드포인트(Device & Endpoint): "어떤 단말에서 접근하는가?"를 판단하는 영역으로, 모든 엔드포인트(PC, 노트북, 모바일, IoT 등)의 무결성과 보안상태를 지속 검증한다.

③ 네트워크(Network): "어떤 경로를 통해 접근하는가?"를 통제하는 영역으로, 전통적인 '내부=신뢰, 외부=비신뢰' 개념을 폐기하고, 네트워크 내 모든 트래픽을 검증 및 암호화를 목표로 한다.

④ 시스템(System): 서버, OS, 미들웨어 등 핵심 인프라 계층의 보안 설정·무결성·운영 안정성 유지 등 인프라 수준에서의 제로트러스트 원칙을 실현한다.

⑤ 애플리케이션 및 워크로드(Application & Workload): "어떤 서비스에 접근하는가?"를 통제하는 영역으로, 사용자·서비스 간 상호작용 시, 애플리케이션이 보안 정책에 따라 동작하는지를 검증한다.

⑥ 데이터(Data): 제로트러스트의 최종 보호 대상으로, 데이터의 생성부터 저장, 전송, 폐기까지 전 생명주기 동안 보호가 이루어져야 한다.

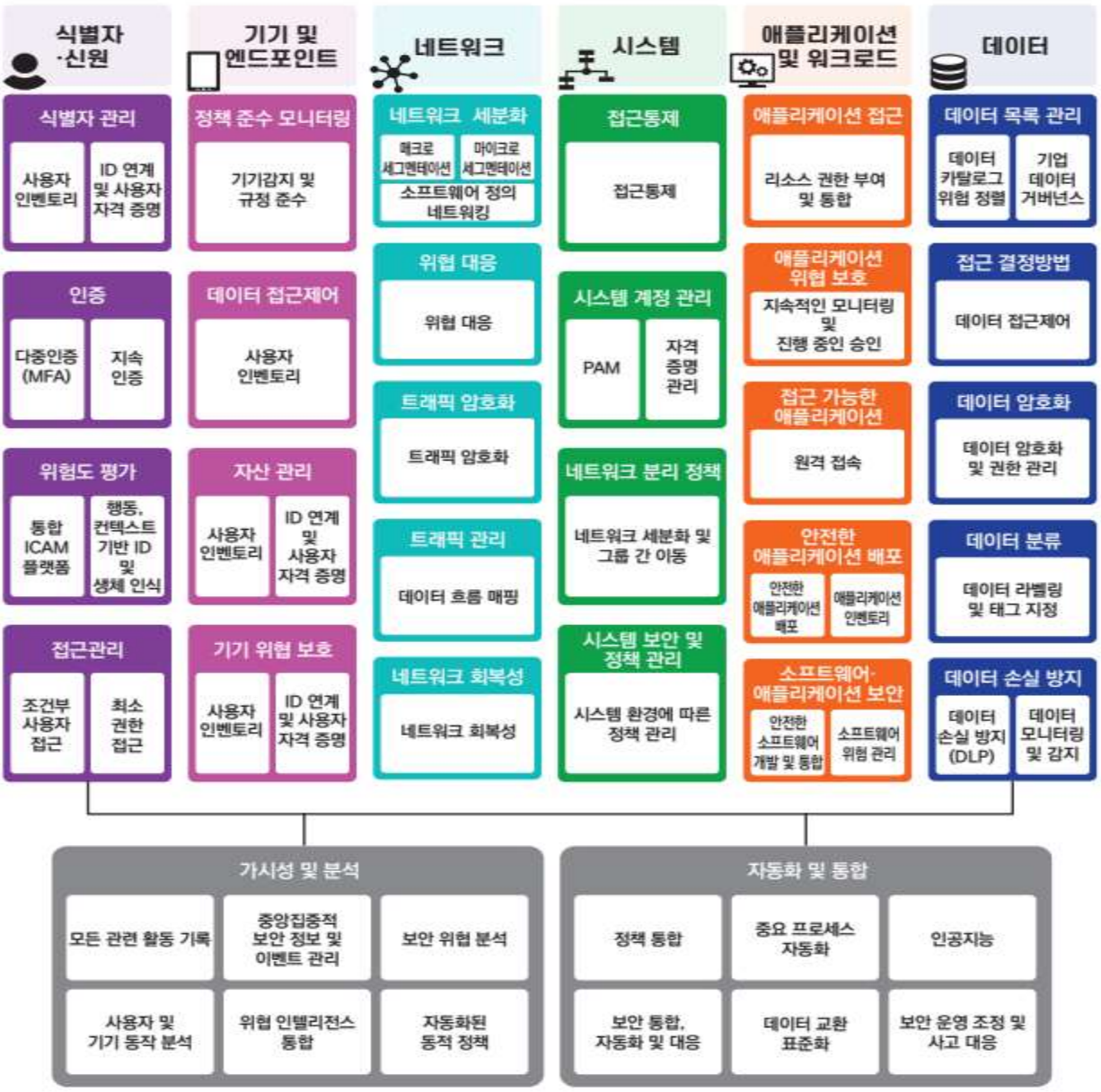
⑦ 가시성 및 분석 (Visibility & Analytics): 조직 전반의 보안 상태, 행위, 위협 흐름을 실시간으로 시각화하고 분석하는 교차 기능으로, "무엇이 일어나고 있는가?"를 파악하기 위한 데이터 기반 의사결정 체계를 지원한다.

⑧ 자동화 및 통합(Automation & Orchestration): 보안 운영 전반을 자동화하고, 다양한 보안 도구와 정책을 통합적으로 오케스트레이션하는 교차 기능으로, "얼마나 빠르고 일관되게 대응할 수 있는가?"를 결정하는 영역이다.

2.2 기능 및 세부역량

제로트러스트 성숙도 모델 2.0에서는 각 핵심 요소별로 가지는 기능을 정의하고, 그 기능별 세부역량을 제시하여 기존 제로트러스트 성숙도 모델의 모호성과 추상성을 극복하고 정보보호 담당자들이 더 명확하고 구체적인 지침을 따를 수 있도록 하였다. **총 27개의 기능(Function)과 52개의 세부역량(Capability)**으로 구성되어 있으며, 그 구조를 요약한 그림은 아래와 같다.

[그림 8] 제로트러스트 핵심 요소/교차 기능별 기능 및 역량



출처: KISA, 제로트러스트 가이드라인 2.0

2.3 역량별 성숙도 수준 체크리스트

제로트러스트 성숙도 평가는 각 요소의 **기능별 세부역량에 대한 396개의 체크리스트**를 통해 수행되며, 전체 요소, 요소별 기능, 기능별 역량에 대한 성숙도 수준 평가 결과를 제공한다. 해당 체크리스트 항목에 대한 상세 설명은 3장 「성숙도 수준 평가를 위한 체크리스트 해설」에서 확인할 수 있다.

[그림 9] 제로트러스트 가이드라인 2.0 성숙도 수준 평가를 위한 체크리스트 – 사용자 인벤토리

세부역량	확인방법	성숙도	Check
사용자 인벤토리	• 사용자 목록에 대한 문서화가 되어있는가?	기존	☐
	• 사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?	초기	☐
	• 자동화된 인벤토리 관리 기구가 도입되어 있는가?	향상	☐
	• 비정상적인 사용자 활동에 대한 탐지가 가능한가?	향상	☐
	• AI 기반 사용자 행동에 따른 관리가 되는가?	최적화	☐
	• 인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?	최적화	☐

출처: KISA, 제로트러스트 가이드라인 2.0

3. 성숙도 수준 평가 요소

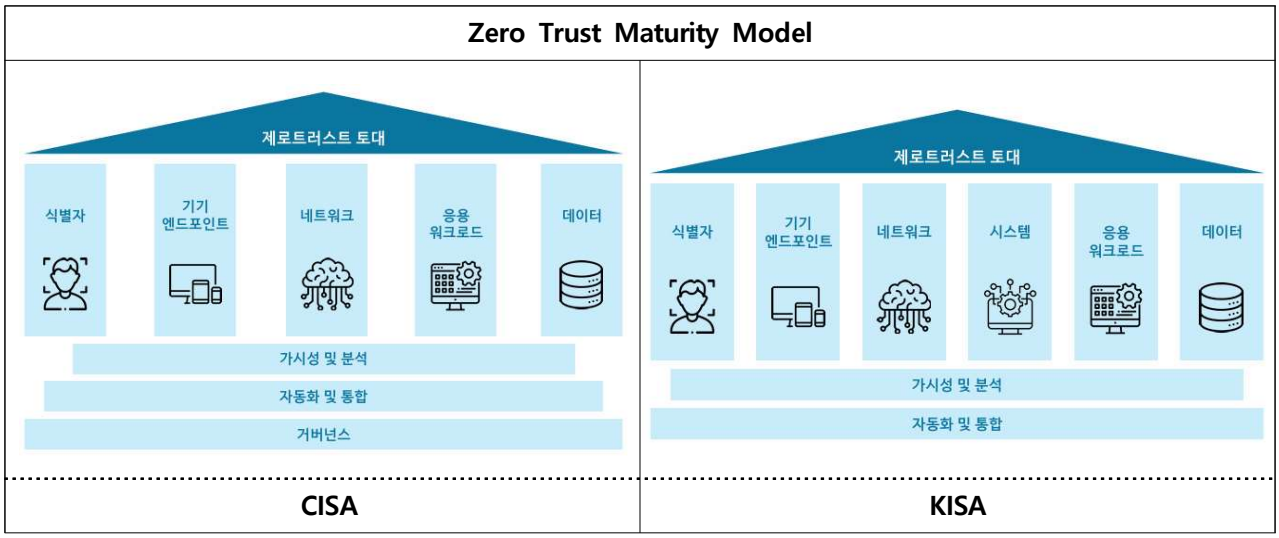
3.1 국내 환경을 반영한 성숙도 평가 요소 구성

제로트러스트 성숙도 모델의 평가 요소는 보안 아키텍처를 구성하는 핵심 요소를 기준으로 정의된다. 디지털 환경이 고도화될수록 사용자가 애플리케이션에 접속하고 데이터에 접근하는 모든 경로에서 보안 위협이 발생할 수 있다. 이에 미국 CISA, DISA/NSA 등은 End-to-End 관점에서 통합적으로 관리하고자 성숙도 수준 평가 요소를 **①식별자(Identity), ②기기 및 엔드포인트(Device & Endpoint), ③네트워크(Network), ④애플리케이션 및 워크로드(Application & Workload), ⑤데이터(Data)**의 5가지 핵심 요소로 구성하였다.

그러나 국내 IT 환경은 시스템 자산이 물리적 혹은 논리적으로 분리되어 운영되며, 재택 및 원격근무와 클라우드 환경의 확산으로 인해 시스템이 독립적인 보호 대상이 되고 있다. 또한 보안 패치 미적용 등으로 인한 시스템 취약점은 기업망 전체에 위협이 될 수 있기에 국내 조직의 특수성과 환경 변화를 반영해 기존 5개 핵심 요소에 **'시스템(System)'을 추가**하였다.

또한 **'가시성 및 분석(Visibility & Analytics)', '자동화 및 통합(Automation & Orchestration)'**은 핵심 요소 전반에 적용되는 교차 기능으로 구성되어 있다. 해당 영역은 위협의 흐름을 실시간으로 시각화하고, 보안 정책을 자동으로 적용하여 고도화된 공격에 신속하고 정확하게 대응할 수 있도록 지원한다.

[그림 10] 제로트러스트 성숙도 모델 구성 요소 비교



3.2 성숙도 수준 평가를 위한 핵심 요소 및 교차 기능 체계

본 해설서는 **6개 핵심 요소**인 ①식별자·신원(Identity), ②기기 및 엔드포인트(Device & Endpoint), ③네트워크(Network), ④시스템(System), ⑤애플리케이션 및 워크로드(Application & Workload), ⑥데이터(Data)와 **2개 교차 기능**인 ⑦가시성 및 분석(Visibility & Analytics), ⑧자동화 및 통합(Automation & Orchestration)을 기준으로 제로트러스트 성숙도 수준 평가 요소를 구분하고 있다.

[표 2] 제로트러스트 핵심 요소별 주요 평가 요소

핵심 요소	핵심 요소 설명	주요 평가 요소
식별자 · 신원 (Identity)	• 사람, 서비스 혹은 IoT 기기 등을 고유하게 설명할 수 있는 속성 또는 속성의 집합 • 강한 인증으로 식별자를 검증하고 세밀한 접근제어(RBAC, ABAC) 규칙에 따라 적절한 시간 내 접근	• 식별자·신원 핵심 요소에서는 사용자를 포함한 개체에 대한 강력한 인증, 통합된 신원관리, 세밀한 접근제어 정책 등의 평가 수행
기기 및 엔드포인트 (Device & Endpoint)	• 기업망에 연결하여 데이터를 주고받는 모든 하드웨어 장치 • MDM 등의 기술을 활용한 기기 신뢰도 평가를 기반으로 신뢰할 수 없는 기기에 대한 접근제어	• 기업 환경에서 사용되는 모든 디바이스의 식별, 등록, 상태관리, 규정 준수 검증 등의 평가 수행
네트워크 (Network)	• 기업망의 유무선 네트워크, 인터넷 등 데이터를 전송하기 위한 모든 형태의 통신 매체 • 네트워크 환경 세분화로 최소한의 권한 부여 및 내외부 데이터 흐름 관리	• 마이크로 세그멘테이션, 암호화된 통신, 세션 기반 접근제어 등의 평가 수행
시스템 (System)	• 온프레미스(On-Premise), 클라우드(Cloud)에 운용 중인 모든 서버 시스템 • 시스템 리소스 접근에 관한 세밀한 접근제어 • 매 세션마다 다중인증(MFA) 등의 신원 확인 및 위험 관리 절차 포함	• 시스템 접근통제, 계정 및 인증 정보 보호, 네트워크 세분화, 시스템 보안 및 정책 관리 등의 평가 수행

애플리케이션 및 워크로드 (Application & Workload)	• 기업망 관리 시스템, 온프레미스(On-Premise), 클라우드(Cloud)에서 실행되는 모든 서비스와 인터페이스 • 응용 계층 및 컨테이너, 가상머신 등을 보호·관리하고 데이터의 안전한 전달	• 애플리케이션 보안, 안전한 개발 및 배포, 워크로드 격리, API 보안 등을 포괄하여 평가 수행
데이터 (Data)	• 최우선으로 보호해야 할 리소스 • 데이터 목록 작성, 분류 및 레이블 지정, 암호화 기법 적용으로 저장 혹은 전송 중인 데이터에 대한 보호 및 데이터 유출 방지	• 데이터 분류 및 라벨링, 암호화, 데이터 손실방지, 접근권한 관리 등의 평가 수행

[표 3] 핵심 요소에 대한 교차 기능별 주요 평가 요소

교차 기능	교차 기능 설명	주요 평가 요소
가시성 및 분석 (Visibility & Analytics)	• 상황에 맞는 세부정보를 이용해 분석하고 가시성 제공 • 비정상 행위에 대한 탐지 개선, 보안 정책 및 접근제어 실시간 처리 • 패킷 단위로 네트워크 트래픽 분석하여 모든 종류의 위협 관찰 및 지능화된 방어 기법 적용	• 모든 활동에 대한 로깅, 실시간 모니터링, 위협 탐지, 사용자 및 개체 행동 분석 등의 평가 수행
자동화 및 통합 (Automation & Orchestration)	• 기존의 수동적인 보안 프로세스를 자동화된 정책 기반 프로세스로 개선하여 신속한 보안 조치 • 자동화된 솔루션 통합으로 일관한 보안 정책 시행 및 자동화된 통합 보안 대응	• 보안 정책의 자동 배포, 위협 대응 자동화, 워크플로우 통합 등의 평가 수행

4. 성숙도 수준 정의

4.1 4단계 성숙도 수준 정의

성숙도 수준은 조직이 **제로트러스트 원칙을 얼마나 충실히 이행하고 있는지 평가하기 위한 기준**으로 보안 정책, 기술 요건, 운영 절차, 보안 문화 등을 포함한 전반적인 이행 상태를 단계적으로 구분한 것이다. 초기 제로트러스트 가이드라인 1.0에서는 성숙도 수준을 '기존(Traditional)', '향상(Advanced)', '최적화(Optimal)'의 3단계로 정의하였으나, 가이드라인 2.0에서는 CISA와 NSA의 최신 모델을 반영해 '초기(Initial)' 단계를 추가한 **4단계 체계**로 재정의하였다.

제로트러스트 성숙도 모델은 조직의 보안 역량과 구현 수준을 네 개의 단계로 구분하여 각 단계별로 달성해야 할 목표와 특징을 명확히 정의하고 있으며, 이러한 단계별 접근은 조직이 자신들의 현재 위치를 정확히 파악하고 체계적인 발전 경로를 설계할 수 있도록 도와준다.

[표 4] 4단계 성숙도 수준 정의

단계	구분	설명
1	**기존** **(정적, 경계기반, 수동)**	• 주요 구성 요소들이 수동으로 설정되며, 정적인 보안 정책으로 인해 유연하지 못하게 정책 시행 • 경계 기반 보안 위주의 보안 아키텍처 구성 • 수동으로 사고에 대응하며, 시스템에 대한 가시성이 제한적
2	**초기** **(일부 자동화)**	• 일부 프로세스가 자동화되며, 핵심 요소별 연계가 일부 이루어짐 • 속성 할당과 생명주기 관리가 부분적으로 자동화되며, 내부 시스템에 대한 기본적인 모니터링 제공 • 프로비저닝 이후 최소 권한 변경에 대응 가능
3	**향상** **(자동화, 중앙 집중적, 통합)**	• 자동화된 범위가 확장되고, 중앙 집중 제어가 강화되는 단계 • 중앙 집중식으로 통합된 가시성 제공 • 중앙 집중식 ID 관리를 통해 핵심 요소 간 상호작용에 기반한 정책 시행
4	**최적화** **(동적, 완전 자동화)**	• 자산 및 리소스에 대한 속성이 완전히 자동으로 할당되며, 동적인 정책이 적용되는 단계 • 자동화된 트리거에 기반한 동적 정책 생성 • 자산에 대해 동적 최소 권한 기반 접근 허용 • 구성요소 간 상호운용성을 위한 개방형 표준 준수 이행 및 강화

성숙도 수준은 조직의 보안 수준을 **정량적으로 평가할 수 있는 객관적인 기준**을 제공한다. 보안 강화가 필요한 영역을 식별하고 자원을 효율적으로 활용하기 위한 근거로써 성숙도 수준이 활용되며, 조직의 현재 제로트러스트 수준을 평가하고 다음 단계로 나아가기 위한 중장기적 로드맵을 마련하는 기반이 된다.

4.2 핵심 요소별 성숙도 수준 정의

[표 5] 핵심 요소별 성숙도 수준 정의

핵심 요소	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자·신원 (Identity)	기존 단계에서는 단일 인증과 역할 기반 접근제어에 의존하지만, 성숙도가 높아질수록 다단계 인증, 위험 기반 적응형 인증, 컨텍스트 기반 접근제어, 행동 분석기반 이상행위 탐지 등 고도화된 기능들이 구현된다. 초기 단계에서는 다단계 인증이 중요 시스템에 제한적으로 적용되며, 향상 단계에서는 조직 전반에 다단계 인증이 확대되고 위험 기반 인증이 도입되며, 최적화 단계에서는 완전히 자동화된 적응형 인증과 지속적인 신뢰 평가를 수행한다.			
	• 온프레미스 ID 사용 • 패스워드 혹은 다중 인증 방식 • 수동접근 및 자격 증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반 인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화 및 동적 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌 ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 허용
기기 및 엔드포인트 (Device & Endpoint)	기존 단계에서는 디바이스 목록 관리가 수동적이고 보안 상태 확인이 제한적이지만, 성숙도가 높아질수록 실시간 디바이스 상태 모니터링, 자동화된 규정 준수 검증, 디바이스 상태에 따른 동적 접근제어가 구현된다. 특히 BYOD 환경에서의 보안 관리, IoT 디바이스 통합관리, 디바이스 신뢰도 점수 산정 등이 고도화 단계의 핵심 기능이다.			
	• 제한된 정책 준수 정보 • 단순하고 수동적 기기 목록 관리 • 수동적 위협 보호 기능 적용	• 대부분의 기기에 정책 준수 시행 메커니즘 사용 • 모든 기기에 대한 목록화 • 기기 보안 솔루션 자동 관리	• 규정 준수 여부에 따른 접근권한 부여 • 검증된 기기만 데이터 접근 • 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	• 지속적인 기기 보안 상태 모니터링 및 검증 • 모든 환경에 결쳐 자산 및 취약점 관리 통합 • 모든 기기에 대해 위협 보호
네트워크 (Network)	전통적인 VLAN 기반 네트워크 분리에서 시작하여, 소프트웨어 정의 경계를 활용한 동적 세그멘테이션으로 발전하며, 최종적으로는 완전히 자동화된 마이크로 세그멘테이션과 제로트러스트 네트워크 접근 아키텍처가 구현된다. 모든 네트워크 트래픽의 암호화, 세션단위 접근 허용, 횡적 이동 차단 등이 중요한 평가 지표이다.			
	• 경계분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그멘트를 통해 엔드포인트 및 애플리케이션 격리 메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위험 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선순위 지정 가능한 동적 네트워크 규칙 생성

핵심 요소	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
시스템 (System)	온프레미스 및 클라우드 환경에 구축 운용중인 서버, 데이터베이스, 운영체제 등 주요 IT 시스템에 대한 세밀한 동적 접근제어와 매 세션마다 다중인증(MFA)과 강력한 신원 확인, 위험관리 절차를 적용하여 시스템의 무결성을 유지해야 한다.			
	• 로컬 시스템 기반 ID/패스워드 등 단순 인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템 보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능	• 동적 접근권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드 (Application & Workload)	성숙도가 높아질수록 DevSecOps 통합, 컨테이너 및 마이크로 서비스 보안, 서비스 메시를 통한 서비스 간 인증 및 암호화, 런타임 애플리케이션 보호 등이 강화된다. 애플리케이션 수준에서의 최소 권한 원칙 적용과 세션별 동적 권한 부여가 핵심이다.			
	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적·수동 테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인, DevSecOps, SBOM적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소 권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협보호에 대한 강력한 통합 • 정기적인 자동화된 테스트	• 실시간 위협 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터 (Data)	데이터 생명주기 전체에 걸친 보호, 민감 데이터의 발견 및 자동 분류, 컨텍스트 기반 데이터 접근제어, 데이터 사용 추적 및 감사 등이 성숙도에 따라 구현된다.			
	• 정적, 수동 데이터 분류 및 접근제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동 데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수도 메커니즘 데이터 분류	• 속성에 기반한 최소 권한 제어 기법으로 접근 관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• AI를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시·최소 권한 동적 데이터 접근 • 사용 중인 데이터 암호화 및 최신 암호화 적용
가시성 및 분석 (Visibility & Analytics)	기본적인 로그 수집과 주기적 검토에서 시작하여, 통합된 SIEM 시스템, 실시간 분석, 머신러닝 기반 이상 탐지, 자동화된 위협 대응으로 발전한다. 성숙도가 높은 조직은 모든 보안 데이터를 상관 분석하여 종합적인 위협 인텔리전스를 생성하고 예측적 보안 운영을 수행한다.			
	• 기본적인 로그 수집 및 모니터링, 분석 지표 정의 • 기본적인 보안 모니터링 수행	• SIEM 구축, 위협 인텔리전스 활용 통합 보안 관제 구현 • 실시간 위협 탐지	• AI, ML 기반 이상 행위 탐지 • 자동화된 위협 헌팅 • 실시간 리스크 평가 체계 운영	• AI 기반 자동화된 동적 정책 시스템 구축 • 자율적 정책 조정 • 자가학습 기반 위협 탐지 • 지능형 위협 분석 • 예측적 보안 분석

핵심 요소	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
자동화 및 통합 (Automation & Orchestration)	수동 프로세스에서 부분적 자동화를 거쳐 완전히 자동화된 정책 관리와 오케스트레이션된 보안 운영으로 발전한다. 거버넌스 교차 기능은 정책 수립, 역할 및 책임 정의, 규정 준수 관리, 지속적인 개선 프로세스 등을 포함한다.			
	• 수동적 정책 적용 • 핵심 보안 및 운영 프로세스 수동 관리 • 정책 조정 시 각각 개별 반영 등 수동적 보안 운영	• SOAR 구축 • 주요 보안 도구 연동 • 기본적인 보안 이벤트에 대한 자동화된 대응	• 정책 통합 시스템 고도화 • 보안 정책 동적 조정 • 주요 보안 이벤트 실시간 대응 • 자동화된 위협 대응 프로세스	• AI, ML 기반 자율적 보안 대응 • 자율 정책 통합 • 지능형 의사결정

4.3 핵심 요소별 기능별 수준 정의

4.3.1 식별자·신원(Identity)

4가지 기능(식별자 관리, 인증, 위험도 평가, 접근관리)으로 구성되며, 상세 내용은 아래와 같다.

<table>
<tr><th>기능</th><th colspan="3">상세</th></tr>
<tr><td rowspan="5">식별자 관리</td><td>설명</td><td colspan="2">• 사용자의 식별 정보를 기반으로 시스템 접근권한을 기록하고 제어
• 사용자 ID, 권한, 역할 등의 정보가 통합·자동화된 방식으로 관리되어야 하며, 최신성과 정확성이 보장되어야 함</td></tr>
<tr><td rowspan="4">성숙단계</td><td>기존</td><td>• 사용자 목록에 대한 문서화
• 사용자 자격 증명에 대한 ID 연계 솔루션 적용</td></tr>
<tr><td>초기</td><td>• 사용자 역할에 따른 상세 인벤토리 구축
• 여러 시스템 간 사용자 자격 증명에 대한 연동</td></tr>
<tr><td>향상</td><td>• 자동화된 인벤토리 관리 기구 도입
• ID 통합 관리 시스템 구축</td></tr>
<tr><td>최적화</td><td>• AI 기반 사용자 행동에 따른 관리
• 글로벌 수준의 ID 연계 기반 통합 사용자 경험 및 프로세스 최적화</td></tr>
<tr><td rowspan="5">인증</td><td>설명</td><td colspan="2">• 시스템 접근 시 사용자를 검증하기 위해 단일 또는 다중 인증 방식으로 접근을 통제
• MFA, FIDO, 지속 인증 등 다양한 수단을 통해 사용자의 신뢰성을 지속적으로 검증함
• 컨텍스트(위치, 장치, 시간 등)에 따라 인증 방식이 동적으로 결정될 수 있어야 함</td></tr>
<tr><td rowspan="4">성숙단계</td><td>기존</td><td>• 단순 MFA(SMS, 이메일 등) 적용
• 세션 기반 인증
• 사용자 행동 및 접속 상태 모니터링 수행</td></tr>
<tr><td>초기</td><td>• 다양한 MFA(인증 앱, 하드웨어 토큰 등) 적용
• FIDO 기반 인증
• 이상행위 탐지 시 추가 인증 수행</td></tr>
<tr><td>향상</td><td>• 컨텍스트 기반 ID 인증
• 동적 인증 기술 기반 실시간 인증 상태 조정</td></tr>
<tr><td>최적화</td><td>• 비정상적 로그인 시도 실시간 탐지 및 대응
• 지속적인 신원 검증</td></tr>
</table>

기능	상세		
위험도 평가	설명	• 사용자, 기기, 권한에 대한 활동 및 상황 정보를 수집하여 위험을 평가하고 인증·접근제어를 강화 • 통합 ICAM 플랫폼을 통해 중앙 집중적 권한 및 식별자 관리를 수행하며, 상황 기반 ID 위협을 실시간 분석함 • 사용자 행동 기반의 생체 인식, 상황 정보(위치, 시간, 장치 등), AI 기반 탐지 기법 등이 함께 활용됨	
	성숙단계	기존	• ICAM 시스템 구축 • 사용자 행동 패턴 수동 분석
		초기	• ICAM 시스템 기반 중앙 집중 관리 및 모니터링 수행 • 컨텍스트 정보 기반 접근권한 조정
		향상	• 보안 기술 및 시스템 통합, 자동화, 위험도 평가 적용을 통한 ICAM 플랫폼 고도화 • 실시간 사용자 행동 및 컨텍스트 변화 반영을 통한 접근제어 조정
		최적화	• AI 기반 ICAM 플랫폼을 통한 보안 강화 • AI 기반 실시간 사용자 행동 분석
접근관리	설명	• 사용자의 위치, 디바이스 상태, 시간 등 다양한 조건에 따라 접근권한을 동적으로 제어 • 역할 기반에서 조건 기반으로 확장되어 최소 권한 원칙을 준수하고 리스크를 줄이는 데 중점 • 리소스·워크로드 단위로 접근 범위를 세분화하고, 정책을 실시간으로 조정할 수 있어야 함	
	성숙단계	기존	• 최소 권한 원칙과 권한 관리 문서화 • 사용자 활동 및 조건 수집을 위한 기초 시스템 구축
		초기	• 조건 기반 접근제어와 권한 관리 표준화 • 시간·위치 기반 최소 권한 원칙에 따른 접근제어, 권한 요청 및 변경 관리 시스템 도입
		향상	• 세션, 리소스 기반 접근제어와 권한 관리 자동화 • 정책 분류·리스트 기반 권한 적용의 체계화
		최적화	• 동적 정책 적용과 권한 변경의 실시간 처리 • AI 기반 사용자 접속 관리

4.3.2 기기 및 엔드포인트(Device & Endpoint)

4가지 기능(정책 준수 모니터링, 데이터 접근제어, 자산관리, 기기 위협 보호)으로 구성되며, 상세 내용은 아래와 같다.

<table>
<tr><th>기능</th><th colspan="3">상세</th></tr>
<tr><td rowspan="5">정책 준수 모니터링</td><td>설명</td><td colspan="2">• 엔드포인트 기기(PC, 노트북, 모바일 등)가 기업의 보안 정책을 준수하고 있는지를 점검·모니터링
• 기기의 운영체제, 보안 설정, 패치 현황 등을 수시로 점검하고, 기준 미달 기기에 대해서는 접근을 제한해야 함
• MDM 등 도구를 활용해 기기 상태를 실시간 확인하고, 정책 위반 시 경고 및 조치가 가능해야 함</td></tr>
<tr><td rowspan="4">성숙단계</td><td>기존</td><td>• 리소스에 연결된 기기 식별
• 규정 준수 수동 평가</td></tr>
<tr><td>초기</td><td>• 실시간 기기 탐지 및 규정 준수 평가
• 규정 비준수 기기에 대한 경고 및 접근 제한</td></tr>
<tr><td>향상</td><td>• 자동 규정 기준 적용
• 규정 준수에 대한 모니터링 및 이에 따른 접근권한 부여</td></tr>
<tr><td>최적화</td><td>• 규정 준수 여부에 따른 동적 권한 수정
• 규정 준수 AI 기반 실시간 평가</td></tr>
<tr><td rowspan="5">데이터 접근 제어</td><td>설명</td><td colspan="2">• 장치가 네트워크에 접근하기 전에 보안 상태(안티바이러스, 무결성 검사 등)를 평가하여, 기준을 만족하는 경우에만 접근을 허용
• NextGen AV, AppControl, FIM 등의 기술을 활용하여 사전 점검을 수행하며, 위험 장치의 접근을 차단함
• 기기 상태에 따라 동적으로 접근권한을 조정할 수 있어야 하며, 타 보안 시스템과 연동된 전략 수립이 필요</td></tr>
<tr><td rowspan="4">성숙단계</td><td>기존</td><td>• 자산 접근 기기에 대한 정보 수집</td></tr>
<tr><td>초기</td><td>• 자산 접근 전 기기에 대한 수동 검사</td></tr>
<tr><td>향상</td><td>• 자산 접근 전 기기 상태에 대한 자동 평가 및 보안 기준 충족 기기만 접근을 허용</td></tr>
<tr><td>최적화</td><td>• 보안 상태에 따른 기기의 접근권한 조정</td></tr>
</table>

기능	상세		
자산관리	설명	• 조직 내 모든 기기(엔드포인트 및 모바일 포함)의 목록을 정확히 작성하고, 보안 상태를 실시간으로 관리 • 기기의 소유자, 위치, 인증 상태, 보안 설정, 패치 현황 등을 중앙에서 통합 관리하여 보안 위협을 사전에 탐지하고 대응함 • 비정상 기기 탐지, 자동 업데이트, 위험 대응 자동화 등을 포함하는 고도화된 관리 체계 필요	
	성숙단계	기존	• 기기 인벤토리 작성 및 수동 업데이트 • 주요 기기에 대한 정보 수집 및 관리
		초기	• 기기 인벤토리 자동화 및 모든 기기 실시간 관리
		향상	• 기기 인벤토리 분석을 통한 보안 취약점 식별 및 비정상적이거나 승인되지 않은 기기 탐지
		최적화	• 실시간 모니터링 및 이상 행위 예측 분석을 통한 기기 관리
기기 위협 보호	설명	• 엔드포인트 기기에서 발생하는 이상행위를 실시간으로 탐지하고, 자동으로 대응 • EDR(Endpoint Detection & Response), XDR(Extended Detection & Response) 솔루션을 활용하여 위협을 식별하고 사전에 차단함 • AI 기반 분석, 자동화된 대응 체계를 통해 실시간 위협 관리가 가능해야 함	
	성숙단계	기존	• EDR 기반의 엔드포인트 위협 탐지 및 초기 대응 정책 수립 • 자산 및 취약성 수동 평가
		초기	• EDR 시스템을 고도화하여 실시간 위협 탐지 및 자동 대응 • 자동화된 취약성 평가 및 패치 관리 도구 도입
		향상	• XDR 기반의 네트워크 전반 위협 탐지 확대 및 정확도 향상 • 모든 자산에 대해 지속적인 취약성 평가 및 패치 관리 자동화
		최적화	• 취약점을 사전에 식별하고 자동으로 패치 적용 • 자산관리, 취약성 평가, 패치 관리 시스템이 통합

4.3.3 네트워크(Network)

5가지 기능(네트워크 세분화, 위협 대응, 트래픽 암호화, 트래픽 관리, 네트워크 회복성)으로 구성되며, 상세 내용은 아래와 같다.

기능	상세		
네트워크 세분화	설명		• 내부 네트워크를 기능, 보안 등급, 사용자 그룹 등에 따라 세분화하여 접근 경로를 제한하고, 공격 확산을 방지 • 마이크로 세그멘테이션을 포함하여 리소스 간 이동을 최소화하며, 공격자가 내부로 침투하더라도 lateral movement(횡적 이동)를 억제함 • 정책 기반 분리, VLAN·보안 도메인 등 다양한 기술을 활용하여 적용 가능
	성숙단계	기존	• 비즈니스 영역별 매크로 세그멘테이션, 자산·트래픽 기반 구성 • 애플리케이션 및 워크로드 기반 마이크로 세그멘테이션, 수동 구성 • SDN 도입 여부, 클라우드 환경 SDN 구조 설정·트래픽 제어 가능
		초기	• 매크로 세그먼트 간 보안 정책 적용, 트래픽 모니터링·이상 탐지 • 애플리케이션 및 워크로드 기반 마이크로 세그먼트 정책 설정, 트래픽 모니터링 가능 • 클라우드 SDN 중앙 관리·실시간 정책 적용
		향상	• 맞춤형 보안 정책 설정, 트래픽 조정 및 위협 대응 가능 • 전체 트래픽 보안 제어, 애플리케이션별 격리 적용 • 클라우드 SDN 확장 통한 트래픽 관리·보안 적용
		최적화	• AI 기반 매크로 세그먼트 관리 적용 • AI 기반 마이크로 세그먼트 관리·자동 대응 • 클라우드 AI 기반 SDN으로 위협 관리·트래픽 예측 가능
위협 대응	설명		• 네트워크 내에서 발생하는 잠재적 위협을 신속히 감지하고 대응 • 침입 탐지 및 방지 시스템(IDS/IPS), 위협 인텔리전스, 자동화된 탐지 및 차단 체계 등을 포함하며, 공격 발생 시 실시간으로 대응함 • 애플리케이션별 트래픽 특성을 파악하고, 이상 징후 탐지 및 정책 기반 대응이 가능해야 함
	성숙단계	기존	• IDS·IPS 기반 위협 감시, 정적 규칙 통한 수동 트래픽 관리
		초기	• 자동 위협 대응 시스템 도입, 앱 프로파일 기반 트래픽 관리
		향상	• 실시간 위협 탐지·선제 대응, 동적 규칙 기반 트래픽 관리
		최적화	• 전사 위협 자동 대응, 앱 프로파일 변화 기반 트래픽 동적 관리
트래픽 암호화	설명		• 네트워크 내·외부를 오가는 데이터의 기밀성을 유지하기 위해 트래픽을 암호화 • SSL/TLS, VPN, 데이터 암호화 및 전송 보안 기술을 활용하여 전송 중인 데이터를 보호함 • 최신 암호화 알고리즘 및 키 관리 시스템을 통해 안정성과 성능을 동시에 확보해야 함
	성숙단계	기존	• 내·외부 트래픽 일부 암호화, SSL/TLS·VPN 사용
		초기	• 전사 암호화 적용, 데이터 전송 암호화 필수
		향상	• 전송·저장 데이터 암호화, 최신 암호화 기술·키 관리 시스템 적용
		최적화	• 최신 암호화·무성능 저하 데이터 보호, 통합 키 관리

기능	상세		
트래픽 관리	설명	• 네트워크 내에서 데이터가 이동하는 경로와 방식을 시각화하고 분석 • 데이터를 주고받는 시스템 간 흐름을 파악해, 데이터 출처, 목적지, 경로 등을 기반으로 보안 정책을 설계하고 위협을 예측할 수 있음 • 실시간 매핑과 이상 흐름 탐지 기능을 포함해 트래픽의 가시성과 우선순위를 동적으로 관리 가능해야 함	
	성숙단계	기존	• 데이터 트래픽 수동 모니터링·흐름 매핑
		초기	• 애플리케이션 단위 트래픽 매핑, 자동화 도구 통한 실시간 데이터 흐름 매핑
		향상	• 데이터 트래픽 보안 정책·이상 탐지, 상관 분석 통한 위협 사전 식별
		최적화	• AI 기반 실시간 데이터 흐름 감지, 트래픽 우선순위 동적 조정
네트워크 회복성	설명	• 네트워크 장애, 공격, 비정상적인 트래픽 증가 등의 상황에서 중단 없이 서비스를 유지하거나 신속하게 복구하는 능력을 확보 • 백업 라우팅, 이중화 경로, 회선 장애 탐지 및 전환, DDoS 대응 체계 등을 포함 • 사전에 설계된 복구 시나리오와 자동화된 대응 정책을 통해 서비스 연속성을 확보해야 함	
	성숙단계	기존	• 애플리케이션 및 워크로드 복구 계획, 주기적 백업·장비 장애 대응 절차
		초기	• 네트워크 다중 경로·이중화 설계, 자동 복구·장애 조치 적용
		향상	• 장애·공격 대응 지속 서비스, 재해 복구 계획 주기적 테스트
		최적화	• 무중단 네트워크 운영, 실시간 장애 감지·자동 복구

4.3.4 시스템(System)

4가지 기능(접근통제, 시스템 계정 관리, 네트워크 분리 정책, 시스템 보안 및 정책 관리)으로 구성되며, 상세내용은 아래와 같다.

기능	상세		
접근통제	설명		• 사용자가 네트워크나 시스템에 접근할 때, 허용된 자원만 사용할 수 있도록 권한을 부여하고 이를 관리 • 권한 기반의 통제를 통해 승인된 사용자만 필요한 리소스에 접근할 수 있도록 하여 내부 오남용이나 침해 사고를 방지함 • RBAC, ABAC 등 다양한 정책 모델을 기반으로 통제 가능
	성숙단계	기존	• 사용자와 기기에 수동 권한 부여 • 역할 기반 접근제어(RBAC) 적용
		초기	• 중앙집중형으로 권한 부여 • 실시간 권한 부여 및 변경 사항 자동 반영 • 특정 리소스에 대한 접근 제한 및 승인 정책 자동 적용
		향상	• 속성 기반 접근제어(ABAC) 적용 • 위치, 기기 상태, 시간 등 기반으로 접근권한 실시간 관리
		최적화	• AI 기반으로 사용자와 기기 상태 실시간 분석 및 자동 권한 조정 • 중앙 시스템 관리 • 시스템 명령 시 신뢰도 재산정 • 위험 분석 기반 지속적 접근제어 정책 도입
시스템 계정 관리	설명		• 권한 있는 사용자 및 시스템 계정에 대한 접근을 통제하고, 인증 정보를 안전하게 저장·관리 • PAM 시스템을 통해 권한 요청·승인·모니터링을 수행하고, 비밀번호·인증서·MFA 등의 자격 정보를 보호함 • 모든 계정과 자격 증명은 중앙에서 일관되게 관리되며, 비정상적인 행위 탐지와 자동 차단 기능이 포함되어야 함
	성숙단계	기존	• PAM 시스템 구축 및 정책 수립 • 자격 증명 수동 관리 • 패스워드 기반 인증 방식 적용
		초기	• PAM 솔루션으로 사용자 접근 모니터링 및 제어 • 자동화된 권한 상승 승인 기술 도입 • 자격 증명 자동 및 중앙 관리 • MFA 등 안전한 인증 방식 적용
		향상	• PAM 솔루션으로 이상행위 탐지 • 생체인증 등 고급 인증 적용 • AI 기반으로 실시간 인증정보 분석
		최적화	• PAM 시스템에 AI 기반 위협 탐지 및 대응 기능 도입 • 비정상 인증 시도 즉각 차단 • 실시간 인증 정책 조정 • 자격 증명 데이터의 중앙 관리 및 시스템 자율화

기능	상세		
네트워크 분리 정책	설명	• 네트워크를 논리적으로 분리하여 각 영역 간 보안을 강화하고, 그룹 간 트래픽 이동을 통제 • 최소 권한 네트워크 접근 원칙을 구현하며, 트래픽 흐름을 제한하고 위협 확산을 방지함 • 보안 정책에 따라 네트워크를 세분화하고, 그룹 간 이동 시 모니터링·검사·제어를 통해 안전한 통신을 보장해야 함	
	성숙단계	기존	• 네트워크 세분화 및 이동 통제 부족 • 망분리 중심의 경계형 네트워크 모델 적용
		초기	• 시스템 중요도에 따른 네트워크 분리 • 제한적 보안 통제 적용으로 네트워크 간 이동 제어
		향상	• 워크로드별 네트워크 세분화로 보안 정책 개별 적용 • 그룹 간 이동 시 강력한 접근통제 및 인증 적용, 실시간 보안 감사 및 트래픽 이동 관리
		최적화	• 그룹 간 이동 시 실시간 분석 및 제어 • 재인증 없는 그룹 간 이동 • 실시간 보안 정책 조정
시스템 보안 및 정책 관리	설명	• 온프레미스와 클라우드 등 이기종 환경에서 일관된 보안 정책을 유지하고, 환경 변화에 따라 보안 정책이 유연하게 조정되도록 관리 • 다양한 환경 전환 상황에서도 보안 수준을 일정하게 유지하기 위해 정책을 자동화하고 정책 적용 범위를 조정할 수 있어야 함	
	성숙단계	기존	• 온프레미스 환경에서 보안 정책 수립 • 수동으로 보안 정책 유지 및 관리
		초기	• 클라우드 환경 전환에 따른 보안 정책의 환경별 수립 • 정책 자동 적용
		향상	• 하이브리드 클라우드 환경 전환에 따른 실시간 보안 정책 조정 • 정책 동적 변경
		최적화	• 보안 위협에 맞는 자율 정책 적용 • 정책 관리의 완전 자동화 및 환경 변화 대응 일관성 유지

4.3.5 애플리케이션 및 워크로드(Application & Workload)

5가지 기능(애플리케이션 접근, 애플리케이션 위협 보호, 접근 가능한 애플리케이션, 안전한 애플리케이션 배포, 소프트웨어 · 애플리케이션 보안)으로 구성되며, 상세내용은 아래와 같다.

기능	상세		
애플리케이션 접근	설명	• 애플리케이션 및 시스템 자원에 대한 접근권한을 통합적으로 관리 • 사용자, 워크로드, 시스템에 대한 최소 권한 원칙을 기반으로 접근을 제어하고, 다양한 조건(위치, 시간 등)을 고려하여 동적으로 권한을 부여함 • 권한 부여·회수, 실시간 위험 기반 제어, 비정상 접근 탐지 등의 자동화가 필수적임	
	성숙단계	기존	• 사용자·시스템 권한 수동 관리, 정적 속성 기반 접근제어
		초기	• 워크로드 접근·리소스 권한 중앙 집중 관리
		향상	• 컨텍스트 기반 최소 권한 접근, 정밀 권한 관리
		최적화	• 실시간 위험·행동 분석 기반 접근, 자동 권한 부여·회수 및 이상 접근 차단
애플리케이션 위협 보호	설명	• 애플리케이션과 시스템의 보안 상태를 자동화된 도구와 프로세스를 통해 실시간으로 모니터링하고, 보안 이벤트 발생 시 즉각 대응 • 시스템 변경 사항에 대한 탐지, 이상 징후 탐색, 보안 승인 프로세스 자동화 등을 포함함	
	성숙단계	기존	• 애플리케이션·시스템 보안 수동 모니터링·이벤트 기록 여부
		초기	• 자동 보안 모니터링·이벤트 분석, 시스템 변경 보안 검토
		향상	• AI 기반 이상 탐지, 보안 승인 프로세스 자동화
		최적화	• 실시간 보안 상태 탐지·위협 사전 예측
접근 가능한 애플리케이션	설명	• 사용자가 외부에서 안전하게 조직 네트워크나 애플리케이션에 접근할 수 있도록 제어 • VPN, 프록시, MFA, IDP 등을 이용하여 기기 및 사용자의 신뢰성을 확인하고 최소 권한 정책에 따라 접근을 통제함 • 원격 환경에서도 애플리케이션 기능 제한, 위험 탐지 및 대응이 가능해야 함	
	성숙단계	기존	• VPN 외부 접속 지원, 애플리케이션 접근제어 제한
		초기	• 원격 기기 보안 자동 평가·접근제어
		향상	• 원격 기기 실시간 모니터링·제어, 맞춤형 보안 정책 수립
		최적화	• 접속 상황 기반 동적 정책 적용, AI 활용 원격 보안 고도화·위험 시 기능 제한

기능	상세		
안전한 애플리케이션 배포	설명	• 조직 내 응용 프로그램의 보안 배포와 식별·관리를 체계화 • 코드 검증, 취약점 검사, 자동화된 배포 파이프라인, 보안 정책 검증 도구 도입 • 모든 애플리케이션의 상태, 위치, 소유자, 사용 목적 등의 정보를 식별하고 통합 관리함	
	성숙단계	기존	• 배포 전 수동 코드 검토·취약점 검사, 보안 가이드 준수·기본 접근제어 적용 • 애플리케이션 인벤토리 수동 목록화·기본 정보 기록
		초기	• 보안 내재 자동 배포 구축, CI/CD 기반 자동 취약점 검사·코드 무결성 확인·환경 격리 • 자동 인벤토리 도구 통한 애플리케이션 식별·관리
		향상	• 배포 전반 모니터링, 보안 정책 자동 검증·이상 활동 대응·구성요소 보안 검사 • 인벤토리에 보안 정보 연계해 애플리케이션 보안 상태 평가·관리
		최적화	• 자동 코드 배포·권한 제어, AI 기반 위협 대응 통합·중앙 관리·자동 보고 • AI 기반 인벤토리 실시간 반영, 보안 시스템 통합 통한 종합 보안 관리
소프트웨어·애플리케이션 보안	설명	• 개발 초기부터 보안 요소를 내재화하여 안전한 소프트웨어를 개발하고, 운영 중 발생 가능한 위협을 식별·평가·대응 • DevSecOps 기반 자동화된 보안 테스트, SBOM 작성, 공급망 보안 강화 등 포함 • 위험 평가 프로세스를 통해 잠재적 취약점을 선제적으로 탐지하고 대응 체계를 갖춤	
	성숙단계	기존	• 보안 코딩 표준 적용, 배포 전 수동 보안 테스트 • 위험 요소 식별·문서화, 위험 관리 계획 수립
		초기	• 보안 내재 개발, DevSecOps 도입, SBOM 작성 • 위험 평가 프로세스 도입·위험 수준 평가
		향상	• 서드파티·오픈소스 보안 검사 자동화, 전반적 SBOM 작성 • 소프트웨어 공급망 보안 강화·전주기 자동 위험 관리
		최적화	• 개발 조직 프로세스 격리, 런타임 소프트웨어 분석 자동화 • AI 예측 분석 통한 위험 식별·맞춤형 공격 대응

4.3.6 데이터(Data)

5가지 기능(데이터 목록 관리, 접근 결정방법, 데이터 암호화, 데이터 분류, 데이터 손실 방지)으로 구성되며, 상세내용은 아래와 같다.

기능	상세		
데이터 목록 관리	설명	• 조직 내 모든 데이터를 식별·분류·카탈로그를 작성하고, 데이터 항목별 민감도·위험도를 분석 • 이를 바탕으로 데이터 사용·보호·관리에 대한 정책을 수립하고 지속적으로 관리함 • 자동화된 도구를 통해 위험 데이터를 탐지하고, 정책 준수 여부를 모니터링함	
	성숙단계	기존	• 데이터 자산의 초기 카탈로그 작성 • 수동적인 데이터 유형 분류 • 데이터 위험 평가 문서화 • 데이터 거버넌스 정책 수립 및 관리에 대한 기본 지침 마련
		초기	• 자동화된 데이터 카탈로그 도구 도입 • 데이터 자산 일부 자동 수립 및 분류 • 위험 수준 평가를 위한 기본 기준 및 지침 마련 • 정책 준수를 위한 감사와 검토의 정기화
		향상	• 데이터 민감도 및 위험 수준 평가 위한 분석 도구 마련 • 데이터 자동화 및 보호 정책 적용 • 데이터 사용 패턴 분석 • 정책 준수 실시간 모니터링
		최적화	• AI 기반 실시간 분석 • 데이터 카탈로그와 보안 시스템 간의 통합 관리 • 조직 전체 시스템과의 데이터 거버넌스 통합 및 일관된 데이터 관리 가능
접근 결정방법	설명	• 데이터를 보호하기 위해, 사용자·장치·NPE 등 주체의 속성에 따라 적절한 데이터 접근권한을 부여하고 통제 • 최소 권한 원칙을 기반으로 접근을 제한하고, 정책 기반의 접근통제를 구성하며, 실시간으로 권한 조정을 수행함	
	성숙단계	기존	• 데이터 접근 정책 수립 • 접근권한 수동 부여
		초기	• 중앙 집중식 접근제어 시스템 도입 • 최소 권한 기반의 데이터 접근 여부 결정
		향상	• ABAC 기반 컨텍스트 접근권한 관리 구현
		최적화	• AI 기반 실시간 권한 조정으로 데이터 접근제어 최소화

기능	상세		
데이터 암호화	설명	• 저장 및 전송 중인 데이터의 무결성과 기밀성을 보호하기 위해 암호화를 수행하고, 접근 권한을 통제 • 정해진 암호화 정책과 권한 체계를 기반으로 데이터 보호를 실현	
	성숙단계	기존	• 데이터 수동 암호화 • 암호화 정책 수립 • 초기 권한 관리 체계 수립으로 데이터 보호
		초기	• 자동화 도구로 중요 데이터 암호화 • 중앙집중식 권한 관리 시스템 도입
		향상	• 고급 암호화 기술 도입 및 권한 관리 시스템과의 통합 관리 • RBAC과 ABAC 결합으로 정밀 권한 관리 구현
		최적화	• AI 기반 암호화 및 권한 관리로 데이터 보호 최적화, 실시간 권한 조정
데이터 분류	설명	• 조직 내 데이터를 민감도, 중요도, 유형 등에 따라 체계적으로 분류하여 보안 정책을 적용 • 데이터 식별·라벨링, 보존 기간 및 삭제 기준 등을 명확히 하여 적절한 보호 조치를 구현함 • 분류 기준에 따라 접근권한 및 관리 체계가 자동으로 적용되어야 함	
	성숙단계	기존	• 라벨링 및 태그 지정 지침 수립 • 일관된 데이터 분류 체계 마련
		초기	• 라벨링 및 태그 수동 지정 • 민감 데이터에 특수 라벨 및 보안 정책 차등 적용
		향상	• 자동화된 라벨링 및 태그 지정 도구로 자산의 자동 분류/식별 • 타 보안 시스템과 연계한 데이터 보호
		최적화	• 고급 메타데이터 관리 도구로 라벨링 및 태그 지정 프로세스 적용 • AI 기반으로 데이터 환경 변화에 실시간 대응하여 자동 분류
데이터 손실 방지	설명	• 민감한 데이터의 무단 유출과 접근을 차단하기 위한 보호 기술 및 정책 • 사전 승인된 DLP 도구를 활용해 데이터 속성 기반 정책 적용 및 모니터링 수행 • 조직 내 업무에 영향 없도록 '모니터링 전용' 모드부터 시작하여 점진적으로 통합	
	성숙단계	기존	• DLP 정책 수립 및 수동 평가 • DLP 도입 위한 기업 내 범위 지정
		초기	• DLP 도구로 주요 데이터 유출 경로 모니터링 • DLP 정책 중앙 관리 • DLP 솔루션의 모니터링 모드 사용
		향상	• DLP 시스템의 전면 도입 및 실시간 데이터 보호, 유출 방지 • DLP 솔루션의 방지 모드 사용
		최적화	• AI 기반으로 데이터 유출 위험의 실시간 예측 및 차단 • 데이터 환경 변화에 따른 보안 정책 자동 최적화

제3장

성숙도 수준 평가를 위한 체크리스트 해설

1. 식별자·신원
2. 기기 및 엔드포인트
3. 네트워크
4. 시스템
5. 애플리케이션 및 워크로드
6. 데이터
7. 가시성 및 분석
8. 자동화 및 통합

1. 식별자 · 신원

1.1 식별자 관리

항목	1.1.1 사용자 인벤토리	
설명	사용자 인벤토리는 시스템에 접근하는 모든 사용자와 그들의 권한을 기록하고 관리하는 시스템이다. 이 기능은 사용자에 대한 정확하고 최신 정보를 제공하여 적절한 접근제어를 가능하게 한다.	
체크리스트	기존	사용자 목록에 대한 문서화가 되어 있는가?
	초기	사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?
	향상	자동화된 인벤토리 관리 기구가 도입되어 있는가?
		비정상적인 사용자 활동에 대한 탐지가 가능한가?
	최적화	AI 기반 사용자 행동에 따른 관리가 되는가?
		인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?

세부 설명

■ **기존**

✓ **사용자 목록에 대한 문서화가 되어 있는가?**

- 시스템 접근이 가능한 사용자 목록을 수집하고 문서화하는 단계로, 주로 수동 방식으로 텍스트 문서나 스프레드시트를 활용해 목록을 관리한다. 사용자 ID, 소속, 이메일 등 기본 정보만 포함되며, 변경사항 반영이 즉각적으로 이루어지기 어려운 상태이다. 실무 환경에서 사용자 목록에 대한 문서화는 조직 소속의 사용자와 외부 협력업체 등 조직의 리소스에 접근 가능한 사용자를 식별하고 문서화하여 이를 활용해 수동으로 보안 정책을 부여할 수 있다.

■ **초기**

✓ **사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?**

- 사용자에게 부여된 역할(Role) 및 권한 수준을 기반으로 정형화된 인벤토리가 구성되는 단계이다. 시스템별 접근권한, 업무 및 역할, 조직 구조 등이 반영되며, 변경 이력과 정기적 검토가 포함된다. 사용자 인벤토리 역할을 할 수 있는 인벤토리 관리 기구(Directory, HRM, IAM 등)를 활용하여 사용자 목록을 관리하며, 사용자(계정)별로 역할(Role)을 부여하여 시스템 기반의 보안 정책을 부여할 수 있다.

■ **향상**

✓ **자동화된 인벤토리 관리 기구가 도입되어 있는가?**

- 사용자 정보가 자동으로 수집·갱신되는 구조로, 인벤토리가 다이렉트 서비스, 인증 시스템, 업무 시스템 등과 연동되어 실시간으로 계정을 관리한다. 입사 또는 퇴사 등 계정 변경 사항 발생에 따라 계정이 자동 생성, 삭제되고 역할에 맞는 권한을 자동으로 부여해야 한다. 사용자 정보의 변경이 생길 시

인벤토리 관리 기구(HRM, Directory, IAM 등) 연동을 통하여 자동화된 연계를 수행한다. 예를 들어 최초 입사자가 인사관리시스템(HRM)에 등록되면 해당 사용자 정보를 통합계정 및 접근관리(Directory, IAM, ICAM)시스템에 자동으로 전달하여 기본적인 보안 정책을 부여해야 한다.

✓ **비정상적인 사용자 활동에 대한 탐지가 가능한가?**

- 상세 인벤토리 정보(사용자 로그인 시간, 위치정보, 디바이스 맥주소 등)를 분석한 후 사용자 이상행위(평소와 다른 접속, 시간, 지역, 접근 요청 등) 및 예외적인 권한 사용, 장기간 미사용 계정을 식별해야 한다. 사용자 활동에 대한 비정상적인 탐지를 할 수 있는 시스템(IAM, ICAM, SIEM, SOAR 등)을 통해 사용자 인벤토리 정보의 정상 행위 기준선을 설정하고 특정 이상 행위를 시나리오, 플레이북 등을 기반으로 탐지할 수 있어야 한다.

■ **최적화**

✓ **AI 기반 사용자 행동에 따른 관리가 되는가?**

- AI 기반 분석 엔진이 사용자 행동을 학습하여 이상 패턴 감지 및 리스크 수준에 따라 자동 조치를 수행하는 단계이다. 정해진 시간, 장소 외 로그인이나 비정상 권한 상승 요청 등을 실시간으로 탐지하여 차단하거나 관리자 알림을 발생시킨다. ML/AI 기반의 사용자 및 엔티티 행동 분석(UEBA) 엔진을 활용하여 각 사용자의 정상적인 활동 패턴을 지속적으로 학습하고, 이상 행위 발생 시 관리자의 개입 없이도 실시간으로 접근을 차단하거나 추가 인증 등을 강제할 수 있다.

✓ **인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?**

- 사용자 인벤토리가 전사 모든 시스템(On-premise, Cloud, SaaS)과 완벽하게 통합되어, 단일 플랫폼에서 사용자(계정)에 대한 권한, 계정 상태, 활동 기록 등을 통합관리하고 제어한다. 통합된 단일 플랫폼을 기반으로, 사용자(계정)별로 사용하지 않는 권한을 자동으로 회수하거나 유사 직무 그룹과의 비교를 통해 권한을 최적화하도록 제안하는 등 사용자 및 권한 관리를 자동화하여 대응할 수 있다.

항목	1.1.2 ID 연계 및 사용자 자격 증명	
설명	여러 시스템 간의 사용자 자격 증명과 인증을 통합하는 프로세스로, 처음에는 ID 생명주기 관리(Identity Lifecycle Management, ILM) 프로세스를 표준화하고, 표준 조직 IDP/IDM 솔루션과 통합하는 데 초점을 맞춘다. 이를 완료한 후, 단일 솔루션이나 ID 연합을 통해 엔터프라이즈 ILM 프로세스/솔루션을 구축하는 것으로 전환된다.	
성숙단계	기존	사용자 자격 증명에 대한 ID 연계 솔루션이 적용되어 있는가?
	초기	여러 시스템 간 사용자 자격 증명에 대한 연동이 되어 있는가?
	향상	ID 통합 관리 시스템이 구축되어 있는가?
	최적화	글로벌 수준의 ID 연계 솔루션이 적용되어 있는가?

세부 설명

■ **기존**

✓ **사용자 자격 증명에 대한 ID 연계 솔루션이 적용되어 있는가?**

- ID 제공자(IDP)와 사용자 디렉터리 간 연계를 통해 기본 인증 방식을 통합하여 하나의 계정을 통해 여러 시스템에 로그인할 수 있다. 인증 정보는 중앙에서 관리되지만, 사용자 자격의 세분화나 권한 제어는 미흡한 단계이다. 실무 환경에서 ID 연계의 예시로, Directory와 SSO 솔루션과 연동하여, 사용자가 Directory 계정 로그인 시 내부 시스템(ERP, 그룹웨어 등)까지 접근할 수 있도록 사용자 자격 증명 정보를 연계할 수 있다. '기존 단계'에서의 ID 연계는 관련된 솔루션 적용 여부만 확인한다.

■ **초기**

✓ **여러 시스템 간 사용자 자격 증명에 대한 연동이 되어 있는가?**

- 인증 프로토콜 표준화를 바탕으로 주요 내부 시스템(ERP, 그룹웨어 등) 간 사용자 계정 정보를 연동, 통합 로그인 환경을 구현한다. 내부 시스템뿐만 아니라 SaaS 등의 외부 시스템까지 인증 방식을 연동하여 다양한 인증 요청을 하나의 자격으로 처리한다. 실무 환경에서는 SAML, OAuth 등과 같은 표준 인증 프로토콜을 기반으로, 사용자 자격 증명에 활용되는 다양한 시스템(HRM, Directory, IAM, ICAM 등) 간의 연동을 수행할 수 있다.

■ **향상**

✓ **ID 통합 관리 시스템이 구축되어 있는가?**

- 다양한 ID 제공자를 통합하여 내/외부 사용자의 구분 없이 하나의 중앙화된 ID 관리 시스템을 통해 모든 사용자 인증 흐름을 제어하고 전사 계정 관리를 수행한다. 시스템 인증 시 암호화가 적용된 프로토콜을 사용하여 보안성을 강화한다. 실무 환경에서는 SAML, OAuth 등과 같은 표준 인증 프로토콜을 기반으로, 사용자 자격 증명에 활용되는 다양한 시스템(HRM, Directory, IAM, ICAM 등) 간의 연동을 수행할 수 있다.

■ **최적화**

✓ **글로벌 수준의 ID 연계 솔루션이 적용되어 있는가?**

- 지역 분산 환경, 다양한 클라우드, 외부 파트너까지 모든 자격 증명이 단일 정책을 기반으로 제어되는 글로벌 단위의 ID 연계 환경을 구축한다. 이러한 정책은 전사 모든 시스템 환경을 고려해야 하며, 환경 변화에 따라 지속적으로 업데이트된다. 실무 환경에서는 본사뿐만 아니라 각기 다른 인프라와 정책을 가진 해외 지사, 그리고 외부 협력사 사용자까지 단일 ID 플랫폼(ICAM 등) 안에서 관리 범위를 확장하여 식별하고 일관된 보안 정책을 적용할 수 있다. 이를 통해 글로벌 거점이나 파트너사가 자체적으로 관리하던 자격 증명까지 중앙 정책 엔진을 통해 제어함으로써, 전사적인 제로트러스트 보안 수준을 유지하고 관리 복잡성을 줄일 수 있다.

1.2 인증

항목	1.2.1 다중인증(MFA)	
설명	사용자가 시스템에 접근하기 위해 두 개 이상의 인증 방법을 요구하는 보안 조치로, 사용자 관리 중앙화를 가능하게 하도록 다중 요소 인증(MFA)과 아이덴티티 제공자(Identity Provider)를 도입하는데 초점을 맞춘다. 성숙도 수준이 높아짐에 따라 대체 가능하고 유연한 MFA 방식을 적용하여 내부 사용자와 외부 사용자에게 접근을 제공하는 데 사용될 수 있도록 한다.	
성숙단계	기존	패스워드와 단순한 MFA(SMS, 이메일)가 같이 적용되어 있는가?
	초기	인증 앱, 하드웨어 토큰 등 다양한 MFA가 구현되어 있는가?
		FIDO 기반 인증 기법이 적용되어 있는가?
	향상	상황에 따른 맞춤형 MFA가 지원 가능한가?
		컨텍스트(단말 위치, 네트워크, 접속 시간 등)를 고려한 ID 인증 방식이 적용되어 있는가?
	최적화	비정상적 로그인 시도를 실시간으로 탐지하고 대응 가능한가?

세부 설명

■ **기존**

✓ **패스워드와 단순한 MFA(SMS, 이메일)가 같이 적용되어 있는가?**

- 가장 기본적인 형태의 MFA 적용 단계로, 단일 시스템이나 솔루션에서 자체적인 MFA 기능을 통해 ID/비밀번호 외의 SMS, 이메일 코드 등의 2차 인증을 수행한다. 실무 환경에서는 그룹웨어나 SSL-VPN 등 특정 시스템에 접속할 때, 해당 시스템이 자체적으로 제공하는 SMS 또는 이메일 기반의 OTP를 추가로 입력하는 상태를 의미한다. 이는 전사적으로 통합 관리되지 않고 개별 시스템 단위로 적용되며, 비교적 보안 강도가 낮은 인증 방식에 해당한다.

■ **초기**

✓ **인증 앱, 하드웨어 토큰 등 다양한 MFA가 구현되어 있는가?**

- 인증 앱, 하드웨어 토큰 등 다양한 인증 수단을 제공하여 보안을 강화한다. 또한 MFA 적용 시스템, 필요 상황, 계정에 따른 인증 방식 차별화 등의 정책을 수립하고 모든 시스템에서 동일한 MFA 요구사항이 적용되도록 표준화한다. MFA 솔루션을 활용하여 동일한 MFA 시스템을 통해서 앱, 하드웨어 토큰 등을 활용할 수 있다.

✓ **FIDO 기반 인증 기법이 적용되어 있는가?**

- FIDO는 '신속한 온라인 인증'을 뜻하는 말 그대로 온라인 환경에서 ID, 비밀번호 없이 생체인식 기술을 활용하여 간편하고 보안성 높은 사용자 인증 서비스를 제공하기 위한 기술이다. Passwordless 도입 단계로 지문, 홍채, 얼굴 인식 등 다양한 생체정보를 활용하여 인증을 수행한다.

■ **향상**

✓ **상황에 따른 맞춤형 MFA가 지원 가능한가?**

- 기기, 위치, IP 등 접속 환경에 따라 MFA를 동적으로 적용한다. 예를 들어, 사내 네트워크에서 접속 시 간단한 인증만을 수행하지만, 외부 네트워크에서 접속 시 강화된 MFA 인증을 적용하는 등 특정 상황에 맞는 조건부 MFA 정책을 적용하여 보안성을 향상시킨다.

✓ **컨텍스트(단말 위치, 네트워크, 접속 시간 등)를 고려한 ID 인증 방식이 적용되어 있는가?**

- 상황에 따른 맞춤형 MFA가 사용자 경험에 초점을 두었다면, 컨텍스트 기반 ID 인증 방식은 보안성 향상에 초점을 둔다. 이는 단말 위치, 네트워크, 접속 시간 등 다양한 컨텍스트 정보를 바탕으로, 평소와 다른 접속 환경이 감지될 경우 인증 수단을 강화하거나 추가 인증을 요구하는 등 동적인 인증을 수행하는 것을 의미한다. 예를 들어, 국내에서만 접속하던 사용자가 해외 IP로 로그인을 시도할 경우, 이를 비정상적인 컨텍스트로 판단하여 추가 인증을 요청하는 방식이 이에 해당한다.

■ **최적화**

✓ **비정상적 로그인 시도를 실시간으로 탐지하고 대응 가능한가?**

- SIEM/SOAR 시스템과 연계하여 비정상적인 로그인 시도를 실시간으로 분석하고 대응한다. 이는 '향상' 단계의 컨텍스트 기반 인증이 확장된 영역으로, UEBA 등의 기술을 활용해 사용자의 평상시 로그인 패턴(접속 시간, 위치, 사용 기기 등)을 학습하고 기준선을 설정한다. 이후 특정 시나리오(예시: 서울에서 로그인 후 10분 이내 뉴욕에서 로그인 시도)나 동일 계정으로 여러 지역에서 동시 접속을 시도하는 등의 이상 행위가 탐지되면, SOAR 플레이북과 연동하여 관리자 개입 없이 자동으로 해당 세션을 강제 종료하거나 즉각적인 MFA 재인증을 요구하는 등 자동화된 실시간 위협 대응을 수행한다.

항목	1.2.2 지속 인증	
설명	제로트러스트가 도입되면 지속적인 속성 기반 인증(Continuous Attribute-Based Authentication)으로 체계적으로 이동할 것이다. 초기에는 기존의 단일 인증을 조직에서 승인된 IDP와 사용자 및 그룹을 기준으로 표준화하는 데 초점을 맞추고, 두 번째 단계에서는 시간 기반의 규칙 기반 인증을 추가하며, 규칙적으로 응용·소프트웨어 활동 및 요청된 권한에 기반한 지속적인 인증으로 발전하게 된다.	
성숙단계	기존	세션 기반 인증이 수행되는가?
		사용자의 행동 및 접속 상태 모니터링이 가능한가?
	초기	이상행위가 탐지되면 세션 중간에 추가 인증하는 시스템이 도입되어 있는가?
	향상	동적 인증 기술을 토대로 실시간으로 인증 상태에 대한 조정이 가능한가?
	최적화	이상 행위 발생 시 자동 재인증 요구, 세션 종료 등 인증에 대한 지속적 검증이 실시간으로 가능한가?

세부 설명

■ **기존**

✓ **세션 기반 인증이 수행되는가?**

- 단순한 연결 기반이 아닌 세션 기반으로 인증을 수행하여 해당 세션 정보를 확인할 수 있다. 세션이 활성화되어 있는 동안은 사용자 신원을 별도로 확인하지 않는 방식으로, 한 번의 로그인 후에는 별도의 추가 인증 없이 시스템 접근이 가능한 형태이다.

✓ **사용자의 행동 및 접속 상태 모니터링이 가능한가?**

- 접속한 세션을 기반으로 사용자의 IP, 접속 시간 등 기본적인 접속 상태를 기록하고 모니터링이 가능하다. 단순 로그 수집 단계로 이상 징후 감지 등의 고도화 기능은 적용되지 않은 상태이다. 단일 시스템(방화벽, SSO 등)에서 세션에 대한 모니터링이 가능하다.

■ **초기**

✓ **이상행위가 탐지되면 세션 중간에 추가 인증하는 시스템이 도입되어 있는가?**

- 사용자 접속 환경에서 IP 주소, MAC 주소, 디바이스 변경 등 사전에 정의된 비정상 행위가 감지되면, 단일 시스템(방화벽, SSO 등) 혹은 MFA 전용 솔루션에서 세션 유지 중간에도 추가 MFA 인증을 요구하여 보안성을 강화한다.

■ **향상**

✓ **동적 인증 기술을 토대로 실시간으로 인증 상태에 대한 조정이 가능한가?**

- SIEM/SOAR 시스템 등과 연계하여 사용자 실시간 데이터를 수집하고 분석할 수 있는 시스템을 구축한 단계이다. 네트워크 변경(예시: 유선에서 무선으로 전환)이 감지될 때 자동으로 재인증을 요청하거나, 사용자 환경 변경(예시: 다른 위치에서의 접속 시도) 시 강화된 인증 또는 소명 처리를 적용하는 등 사용자의 실시간 인증 상태를 바탕으로 동적 인증을 수행한다.

■ **최적화**

✓ **이상 행위 발생 시 자동 재인증 요구, 세션 종료 등 인증에 대한 지속적 검증이 실시간으로 가능한가?**

- 사용자의 모든 접속과 권한 요청을 지속적으로 모니터링하고, 이상 행위가 감지되면 자동화된 인증 관리 체계를 바탕으로 세션을 자동 종료하거나 즉각 재인증을 요구하는 등의 동적 인증을 수행한다. 머신러닝과 AI 등의 기술을 활용하여 이상 행위에 대한 시나리오를 자동으로 업데이트하여 재인증 절차나 세션 종료 등에 대한 조치를 동적으로 반영할 수 있다.

1.3 위험도 평가

항목	1.3.1 통합 ICAM 플랫폼	
설명	통합 ICAM(Identity, Credential, and Access Management) 플랫폼은 식별자, 자격 증명, 접근 관리 기능을 중앙에서 통합하여 관리하는 시스템이다. 엔터프라이즈 수준의 식별자 관리 및 공개 키 인프라(PKI) 시스템을 활용하여 네트워크 전반에 걸쳐 사용자, 관리자 및 NPE(Non-Person Entity) 시 식별자를 추적하고, 접근이 필요한 자와 적절한 권한을 가진 자로 제한되도록 보장하여야 한다. 조직은 자격 증명 관리 시스템, 식별자 거버넌스 및 관리 도구, 접근 관리 도구를 통해 접근권한이 필요하고 적절한지 검증하여야 한다.	
성숙단계	기존	ICAM 시스템이 구축되어 있는가?
	초기	ICAM 시스템 기반 중앙 집중 관리 및 모니터링이 되는가?
		사용자 인증 및 접근 관리에 대한 정책이 표준화되어 있는가?
		사용자 및 권한 관리에 대한 기본적인 위험도 평가가 도입되었는가?
	향상	다양한 보안 기술 및 시스템 통합으로 ICAM 플랫폼이 안정화되었는가?
		ICAM 플랫폼이 자동화되어 있는가?
	최적화	AI 기반의 ICAM 플랫폼을 통해 보안 강화가 이루어지는가?
		실시간 분석을 통한 ID 위험 평가가 이루어지는가?

세부 설명

■ **기존**

✓ **ICAM 시스템이 구축되어 있는가?**

- ICAM 시스템이 도입되기 전 단계로, 일반적으로 Directory, EAM, IM 솔루션 등의 개별 도구를 통해서 사용자를 관리하며 기본적인 수준의 자격 증명과 계정 및 권한 관리가 수행된다. 최소한의 사용자/자격 관리만 수행하는 수준으로 중앙집중화 및 통합관리 기능은 제한적이다.

■ **초기**

✓ **ICAM 시스템 기반 중앙 집중 관리 및 모니터링이 되는가?**

- ICAM 플랫폼이 중앙 집중화되기 시작하는 단계로, IAM 등 시스템을 통해 모든 사용자의 계정과 접근권한을 단일 플랫폼에서 관리하며 모니터링을 수행한다. 모든 로그인, 인증, 권한 부여 요청이 중앙 플랫폼을 거치게 되어 보다 일관된 정책 적용과 로그 확보가 가능하다.

✓ **사용자 인증 및 접근 관리에 대한 정책이 표준화되어 있는가?**

- IAM 등 시스템에서 정의된 계정별 접근권한을 바탕으로 통합인증(SSO) 시스템을 활용해 사용자를 인증한다. 이 단계에서는 인증 방식(MFA 적용 기준, 비밀번호 정책 등)과 권한 부여 방식에 대한 기업 내 표준 정책이 수립 및 문서화 되어 있으며, 이를 통해 모든 사용자에게 일관된 접근 정책을 적용하기 시작한다.

✓ **사용자 및 권한 관리에 대한 기본적인 위험도 평가가 도입되었는가?**

- 사용자 접속 위치, 기기 정보 등 ICAM을 통해 모니터링되고 있는 정보를 바탕으로 사용자 및 권한 관리에 대한 위험도 평가를 수행한다. 도입 초기 단계인 만큼 평가 결과에 대한 조치는 주로 수동으로 수행된다.

■ **향상**

✓ **다양한 보안 기술 및 시스템 통합으로 ICAM 플랫폼이 안정화되었는가?**

- ICAM이 SSO, EDR, DLP, SIEM/SOAR 등 여러 보안 시스템과 연동되어 실시간으로 사용자 정보 및 위험 데이터를 주고받는다. 예시로 EDR를 통해 사용자 PC에서 악성코드가 탐지하면 해당 사용자 권한이 ICAM을 통해 즉시 제한되거나 MFA가 요구되는 등 ICAM이 다른 보안 인프라와 유기적으로 연계되어 실시간 보안 대응 체계를 구축한다.

✓ **ICAM 플랫폼이 자동화되어 있는가?**

- ICAM 내 기능이 자동으로 수행되는 단계이다. 사용자의 계정과 권한이 라이프사이클에 맞춰서 계정 생성/폐기, 권한 부여/회수 등의 자동화가 반영되어 있으며, 계정과 권한에 대한 지속적인 감사를 수행하여 필요 없는 계정과 권한을 삭제 관리 할 수 있다. 보안 시스템과 연동되어 이상 행위 탐지에 따른 보안 대응을 자동으로 수행함으로써 전반적인 사용자/계정 관리 수행에 있어 수동 개입을 최소화한다.

■ **최적화**

✓ **AI 기반의 ICAM 플랫폼을 통해 보안 강화가 이루어지는가?**

- ML/AI 기반 기술이 접목되어 사용자 행동 분석, 권한 이상 탐지, 실시간 리스크 예측 등의 보안 고도화가 이루어진다. 학습된 데이터 기반으로 사용자의 평소 행동과 다른 패턴이 발견되면 자동으로 계정을 제한하거나 강화된 인증을 수행하는 등 전사 보안의 핵심 조정 엔진으로 작동하며, 예측되는 위험이 있으면 정책을 자동으로 조정하고 개선하는 등 보안 사고를 미연에 방지하는 역할을 수행한다.

✓ **실시간 분석을 통한 ID 위험 평가가 이루어지는가?**

- AI를 활용하여 실시간 사용자의 계정과 권한을 분석하고, 타 보안 시스템과 연동된 정보를 기반으로 사용자에 대한 동적인 리스크 점수를 실시간으로 산출한다. 해당 점수를 기반으로 접근 허용 또는 제한 여부를 판단하는 위험 평가를 수행하며, 평가 결과에 따라 접근 차단이나 추가 인증 등의 자동화된 조치를 반영한다.

항목	1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식	
설명	사용자의 행동 패턴, 상황적 정보를 생체 데이터를 활용하여 인증 및 접근제어를 강화하는 기술이다. 엔터프라이즈 IDP를 활용하여 기본 사용자 속성으로 사용자 및 개체 행동 분석(User and Entity Behavioral Analytics, UEBA)을 활성화한다. UEBA를 PAM 및 JIT/JEA 시스템과 통합하여 이상행위 및 악의적인 활동을 보다 효과적으로 탐지할 수 있다.	
성숙단계	기존	기본적인(지문, 얼굴인식) 생체 인식 기술이 적용되어 있는가?
		사용자 행동 패턴이 수동으로 분석되는가?
	초기	행동 및 생체 인식 기술을 통합하여 인증이 가능한가?
		컨텍스트 정보 기반 접근권한이 조정되는가?
	향상	실시간 사용자 행동 및 컨텍스트 변화 반영으로 접근제어 조정이 가능한가?
	최적화	AI 기반 행동 분석 및 생체 인식 솔루션이 도입되어 있는가?

세부 설명

■ **기존**

✓ **기본적인(지문, 얼굴인식) 생체 인식 기술이 적용되어 있는가?**

- 지문, 얼굴 인식, 홍채 스캔 등 전통적인 생체 인식 기술이 일부 도입되어 있는 상태이다. 실무 환경에서는 이러한 기술이 전사적으로 통합 관리되지 않고, 특정 시스템(예시: 근태관리, 출입통제 시스템)에 개별적으로 적용되거나, 생체 인식 기능이 탑재된 일부 사용자 단말기(예시: 특정 모델의 노트북)에서만 제한적으로 활용되는 수준을 의미한다.

✓ **사용자 행동 패턴이 수동으로 분석되는가?**

- 사용자의 로그인 시각, 접속 위치와 같은 행동 패턴 및 상황적 정보가 로그 형태로 수집되지만 자동화된 분석 도구는 도입되지 않은 상태이다. 담당자가 개별 시스템에서 수동으로 로그를 수집하고 분석하며, 통계형 보고서 수준에서 사후에 행동 패턴을 확인할 수 있다.

■ **초기**

✓ **행동 및 생체 인식 기술을 통합하여 인증이 가능한가?**

- 단일 시스템이나 솔루션이 자체적으로 제공하는 SMS, OTP 인증 외에, MFA 솔루션을 활용하여 지문, 얼굴인식 등의 생체 인식 기술을 통합함으로써 인증 절차를 강화한다. 또한, MFA 시스템 기능을 활용하여 사용자 행동 패턴 기반의 강화된 MFA를 적용할 수 있다.

✓ **컨텍스트 정보 기반 접근권한이 조정되는가?**

- 시간, 위치, 장치, 상태, 네트워크 등 기본적인 컨텍스트 데이터를 기반으로 로그인 요청의 위험 수준을 평가한다. 이 단계에서는 정적인 규칙을 기반으로 위험도를 평가하며, 평가된 위험도에 따라 접근 가능한 시스템을 제한하거나 접근권한 자체를 제한하는 등의 조정을 수행한다.

■ **향상**

✓ **실시간 사용자 행동 및 컨텍스트 변화 반영으로 접근제어 조정이 가능한가?**

- 사용자 행동 및 패턴의 실시간 변화를 탐지하여 동적으로 접근을 제한하거나 재인증을 요구한다. 사용자 행동 분석을 위한 UEBA 시스템을 통해 사용자별 엔티티(Entity)를 생성하여 컨텍스트 변화를 감지할 수 있다. 이렇게 생성된 사용자 엔티티 정보는 PAM 시스템과 연동되어 고도화된 접근제어에 활용될 수 있다. 또한, UEBA 시스템을 통해 엔티티가 생성 및 관리되면 JEA(Just-Enough-Access) 기술을 통해 업무에 필요한 최소한의 권한만 부여하고, JIT(Just-In-Time) 기술을 통해 필요시에만 권한을 부여하는 동적인 접근제어 조정이 가능하다.

■ **최적화**

✓ **AI 기반 행동 분석 및 생체 인식 솔루션이 도입되어 있는가?**

- ML/AI를 기반으로 사용자의 행동 패턴, 입력 습관(타이핑 속도, 마우스 이동 등), 생체정보 등을 결합하여 사용자별 엔티티를 고도화한다. 고도화된 엔티티에 새로운 기술을 지속적으로 도입하여 편의성을 저하하지 않으면서 보안을 고도화할 수 있는 방안(별도의 추가 인증 없이 입력 습관을 통해 사용자를 검증하는 등의 방식)을 지속적으로 적용한다.

1.4 접근 관리

항목	1.4.1 조건부 사용자 접근	
설명	사용자의 위치, 디바이스 상태, 시간대 등 다양한 조건에 따라 접근권한을 동적으로 조정하는 기능이다. 연합된 ICAM(Identity, Credential, and Access Management) 전반에 걸친 전통적인 역할 기반 접근제어에서 시작하여, 응용 중심의 역할로 확장되며, 궁극적으로는 동적 접근 규칙을 제공하기 위해 엔터프라이즈 속성을 활용한다.	
성숙단계	기존	사용자 활동 및 조건을 수집할 수 있는 기초 시스템을 구축하였는가?
		조건부 접근 정책에 대한 개념을 정의하였는가?
		시스템별 각기 다른 접속 관리 기능이 있는가?
	초기	특정 조건에 따른 사용자 접근제어가 가능한가?
		시간, 위치 기반으로 최소 권한 원칙에 따른 접근제어가 가능한가?
	향상	세션별 접근권한 부여가 가능한가?
		조건을 정교하게 나누어 다단계 접근 정책이 적용되어 있는가?
		리소스별 접근권한 부여가 가능한가?
	최적화	동적 접근 정책을 실시간으로 적용 가능한가?
		AI 기반 실시간 상황 파악을 통한 사용자 접속 관리가 가능한가?

세부 설명

■ **기존**

✓ **사용자 활동 및 조건을 수집할 수 있는 기초 시스템을 구축하였는가?**

- 단일 시스템이나 솔루션 자체의 기본 로그 수집 시스템을 활용하여 사용자 로그인 시간, IP 주소, 기기 상태 등을 수집할 수 있는 단계이다. 수집된 데이터는 중앙에서 통합 관리되지 않으며, 주로 시스템별로 분산되어 운영된다.

✓ **조건부 접근 정책에 대한 개념을 정의하였는가?**

- 조직의 특성을 반영하여 조건부 접근 정책을 수립하고 문서화한다. 이 단계에서는 '위험 기반' 또는 '컨텍스트 기반' 인증이 무엇인지, 그리고 어떤 상황(예시: 외부 환경에서 내부 네트워크에 접근하는 경우)에 적용되어야 하는지에 대한 기본 개념과 원칙을 내부 보안 지침서 등에 정립한다.

✓ **시스템별 각기 다른 접속 관리 기능이 있는가?**

- 접속 관리 기능이 중앙화되어 있지 않은 상태로, 실무 환경에서 그룹웨어, 파일 서버, 단일 시스템 등 각 개별 시스템이 자체적인 인증 및 권한 관리 기능을 별도로 운영한다. 이로 인해 전사적으로 일관된 접근 정책을 적용하기 어렵고, 통합적인 사용자 권한 현황을 파악하기 어렵다.

■ **초기**

✓ **특정 조건에 따른 사용자 접근제어가 가능한가?**

- 인증 및 접근 계정권한이 중앙집중화되기 시작하며, SSO, IAM 시스템 등을 통해 통합 관리된다. '기존' 단계에서 문서로만 존재하던 조건부 접근 정책이, SSO, IAM 등의 시스템 정책 엔진에 실제 규칙으로 반영되기 시작한다. 사용자 역할이나 기본적인 컨텍스트 확인에 따라 접근 허용 여부를 정책에 반영하고, 이를 기반으로 특정 조건에 따른 접근제어를 수행한다.

✓ **시간, 위치 기반으로 최소 권한 원칙에 따른 접근제어가 가능한가?**

- 사용자 위치, 네트워크 상태, 로그인 시간 등 사전에 정의된 정적 조건(컨텍스트)에 따라 접근을 허용하거나 제한하는 정책을 시스템상에 반영하여 최소 권한 원칙을 적용한다. 실무 환경에서는 중앙집중화된 SSO, IAM 등의 시스템에서, 단순히 시스템 전체의 접근을 허용/차단하는 것을 넘어, 사용자의 컨텍스트에 따라 사전에 정의된 '역할(Role)'을 기반으로 차등 부여하는 것을 의미한다. 예를 들어, 동일한 인사팀 사용자라도 '업무 시간(09:00-18:00)' 중 '사내 IP'에서 접속할 때는 '인사DB 읽기/쓰기' 권한을 부여하고, '업무 시간 외' 또는 '외부 IP'에서 접속할 때는 '읽기 전용' 권한만 부여하는 식으로 시간과 위치 조건에 따라 권한을 최소화할 수 있다.

■ **향상**

✓ **세션별 접근권한 부여가 가능한가?**

- 사용자가 조직 리소스에 접근 이후 생성된 각 세션 자체를 개별적으로 식별하고 모니터링하고 개별적으로 접근권한을 부여할 수 있는지를 의미한다. 실무 환경에서는 동일한 사용자가 여러 기기(예시: 사내 PC와 개인 모바일 태블릿)에서 동시에 접속하더라도, 각 세션을 별도로 식별하여 PC로 접근한 세션에는 '전체 기능'을 허용하고, 상대적으로 보안이 취약할 수 있는 모바일 세션에는 '읽기 전용' 권한만 부여하는 등 세션 단위의 차등적인 접근제어를 수행할 수 있다.

✓ **조건을 정교하게 나누어 다단계 접근 정책이 적용되어 있는가?**

- 사용자 신뢰도, 디바이스 보안 상태, 네트워크 환경, 접속 시간 등 다양한 컨텍스트를 정교하게 세분화하고 이를 조합하여 단계별 접근 정책을 적용한다. 예를 들어, 동일한 사용자라도 1단계('사내망' + '보안 등록 기기' + '업무 시간')로 접속 시에는 기본 인증(ID/PW)만으로 접근을 허용하지만, 2단계('외부망' + '보안 등록 기기') 접속 시에는 MFA(다중인증)를 추가로 요구하고, 3단계('외부망' + '미등록 기기') 접속 시에는 접근 자체를 차단하는 등, 전사적으로 여러 조건의 조합에 따라 인증 강도와 접근권한이 차등 적용되어 있다.

✓ **리소스별 접근권한 부여가 가능한가?**

- 리소스의 중요도에 따라 세분화된 접근제어를 수행하는 것으로, 애플리케이션 내부의 특정 버튼과 화면, 데이터 단위까지 제어하여 접근권한을 차등 부여할 수 있다. 실무 환경에서는 IAM, ZTNA 등의 시스템을 통해서 동일한 사용자라도 특정 애플리케이션에서 '고객 정보 조회'는 가능하지만 '고객 정보 다운로드' 기능은 차단하거나, '주요 데이터'에 접근할 때는 추가 인증(MFA) 등을 요구하는 등 리소스별로 세분화된 접근제어를 수행한다.

■ **최적화**

✓ **동적 접근 정책을 실시간으로 적용 가능한가?**

- ML/AI을 기반으로 사용자 행동, 환경에 따른 위험을 분석하고 각 상황에 따른 사용자 및 기기, 상황별 속성을 정의하여 자동으로 조건을 세분화한다. 이러한 조건은 실시간으로 정책 엔진에 반영되어 동적 접근 정책을 수행한다.

✓ **AI 기반 실시간 상황 파악을 통한 사용자 접속 관리가 가능한가?**

- ML/AI 분석 엔진이 사용자의 행동 패턴(예시: 타이핑 속도, 마우스 이동), 세션 중 활동(예시: 평소와 다른 명령어 사용, 대량의 데이터 접근 시도), 기기/네트워크 상태 변화 등 모든 상황별 속성을 지속적으로 분석하여 동적인 위험 점수를 실시간으로 스코어링 한다. 조건부 정책 엔진은 이 위험 점수가 사전에 정의된 임계치를 초과하거나 기존 정책을 위반할 경우, 관리자의 개입 없이도 즉각적인 조치를 수행한다. 예를 들어, 실무 환경에서는 AI가 '비정상적인 대량 데이터 다운로드 시도'를 탐지하면, SOAR 플레이북 등과 연동하여 해당 세션을 강제 종료시키거나, 사용자의 권한을 실시간으로 '읽기 전용'으로 하향 조정하는 등의 고도로 자동화된 사용자 접속 관리를 수행하는 것을 의미한다.

항목	1.4.2 최소 권한 접근	
설명	사용자가 수행하는 작업에 필요한 최소한의 권한만 부여하여, 타 리소스 및 워크로드에 대한 접근을 제한하는 방식이다. 이를 통하여 리소스 탈취 등을 최소화할 수 있다.	
성숙단계	기존	최소 권한 원칙에 대한 정의가 이루어져 있는가?
		권한 부여에 대한 절차가 문서화되어 있는가?
	초기	권한 부여 절차가 표준화되어 있는가?
		권한 요청 및 변경 관리 시스템이 도입되어 있는가?
	향상	자동화된 권한 상승이 가능한가?
		권한 관리 정책이 지속적으로 업데이트 되는가?
	최적화	권한 관리가 동적으로 변경 가능한가?
		최소 권한 원칙이 실시간으로 조정 가능한가?

세부 설명

■ **기존**

✓ **최소 권한 원칙에 대한 정의가 이루어져 있는가?**

- 조직 내부적으로 사용자가 자신의 역할을 수행하는데 필요한 최소한의 권한만을 시스템 상에서 수행 가능하도록 보장하는 최소 권한 원칙을 정의한다. '최소'의 정의를 위해 업무 프로세스, 필요 리소스 및 기존 권한 등에 대한 상세한 분석을 수행하고 각 역할에 따른 필수불가결한 권한을 확인한다.

✓ **권한 부여에 대한 절차가 문서화되어 있는가?**

- 정의된 최소 권한 원칙 적용을 위해 권한 요청, 승인, 부여, 변경, 회수에 이르는 일련의 프로세스를 문서화한다. 해당 문서에는 권한을 요청하는 사람, 이를 검토하고 승인하는 책임자 등 각 단계의 역할과 책임이 정의되어 있다.

■ **초기**

✓ **권한 부여 절차가 표준화되어 있는가?**

- 모든 부서와 시스템에 걸쳐 동일하게 적용되는 표준화된 권한 부여 절차를 수립한다. 실무 환경에서는 이메일이나 구두로 요청하는 대신, 그룹웨어나 전자 결재 시스템을 통해 모든 권한 요청/승인이 이루어짐을 의미한다. 일반적으로 직무에 따라 역할(Role)과 권한을 매핑한 역할-권한 매트릭스를 정의하고, 이를 기반으로 하는 RBAC(역할 기반 접근제어)를 구현하기 시작한다.

✓ **권한 요청 및 변경 관리 시스템이 도입되어 있는가?**

- 권한 요청 및 변경 이력을 관리하기 위한 그룹웨어, 사용자 포털 등의 시스템이 도입되어, 실무 환경에서는 사용자가 해당 시스템을 통해 권한을 신청하고, 관리자는 이 시스템을 통해 승인/반려 처리를 수행한다. 이러한 모든 승인 및 변경 내역은 시스템적으로 기록되어, 누가, 언제, 어떤 권한을, 누구의

승인을 받아 획득했는지에 대한 감사 추적성을 확보한다. 이는 최소 권한 원칙이 절차에 따라 준수되고 있음을 검증하는 기본 증적이 된다.

■ **향상**

✓ **자동화된 권한 상승이 가능한가?**

- JIT(Just-In-Time) 기술과 같은 자동화된 권한 상승 기능이 구현된 단계이다. 실무 환경에서는 사용자가 특정 서버 관리나 데이터베이스 작업 등 일시적으로 높은 권한이 필요한 업무를 수행하기 위해 권한을 요청할 경우, PAM 또는 IAM 등의 시스템이 사전에 정의된 조건(예시: 승인된 그룹웨어 작업 티켓 연동, 업무 시간 내 요청 등)을 자동으로 검증한다. 조건에 부합하면 시스템은 일시적으로 권한을 부여(상승)하고, 작업이 종료되거나 설정된 시간이 만료되면 해당 권한을 자동으로 회수한다.

✓ **권한 관리 정책이 지속적으로 업데이트 되는가?**

- 권한 관리 정책이 조직의 변화에 맞춰 지속적으로 검토되고 최신화된다. 실무 환경에서는 인사시스템과 IAM 시스템 등을 연동하여, 부서 개편이나 직무 변경과 같은 인사 정보가 발생할 때마다 RBAC의 '역할-권한 매트릭스'를 자동으로 업데이트하거나 관리자에게 검토 알림을 보낸다. 또한, 분기별 또는 반기별로 정기적인 권한 재검토 프로세스를 시스템을 통해 수행하여, 사용자가 현재 보유한 권한이 여전히 업무에 필요한지를 검증하고 불필요한 권한을 체계적으로 회수한다.

■ **최적화**

✓ **권한 관리가 동적으로 변경 가능한가?**

- ML/AI을 기반으로 사용자 행동, 기기 상태, 네트워크 트래픽, 위협 인텔리전스 등 다양한 컨텍스트를 실시간으로 분석하여 동적인 위험 점수를 실시간으로 스코어링 한다. 이 점수는 ICAM 시스템 등의 정책 엔진에 즉각적으로 반영되어, 사용자의 업무 활동과 실시간 스코어링 된 점수 수준에 따라 권한이 동적으로 상향 또는 하향 조정되는 동적 접근 정책을 수행한다.

✓ **최소 권한 원칙이 실시간으로 조정 가능한가?**

- 정책 엔진에 JIT(Just-In-Time) / JEA(Just-Enough-Access) 기술이 적용되어 권한 변동이 발생하면 필요한 권한을 일시적으로 부여하고 자동으로 회수한다. 실무 환경에서는 ML/AI을 활용하여 산출한 동적인 위험 점수와 사용자의 실시간 요청을 기반으로, 정책 엔진이 JIT/JEA 기술을 통해 필요한 최소한의 권한(JEA)을 필요한 시간(JIT)만큼만 자동으로 부여한다. 예를 들어, 개발자가 평소 접근하지 않던 운영 서버에 긴급 패치 작업을 위해 접근을 요청할 경우, 정책 엔진이 해당 작업의 정당성(예시: IAM 시스템 연동)과 사용자의 위험 점수를 실시간으로 스코어링하여, PAM 시스템을 통해 2시간 동안만 해당 서버의 '패치 실행' 명령어 권한(JEA)을 부여하고 시간이 만료되면 자동으로 회수한다. 이를 통해 상시 존재하는 특권(Standing Privilege)을 제거하고 자율적으로 최소 권한 원칙을 실시간 조정한다.

2. 기기 및 엔드포인트

2.1 정책 준수 모니터링

항목	2.1.1 기기 감지 및 규정 준수	
설명	네트워크에 연결된 장치가 조직의 보안 규정을 준수하는지 확인하고, 비준수 장치를 탐지하여 경고하는 시스템이다.	
성숙단계	기존	리소스에 연결된 기기를 식별할 수 있는가?
		수동으로 규정 준수에 대한 확인이 가능한가?
	초기	실시간으로 기기를 탐지하고 규정 준수를 평가할 수 있는가?
		비준수 기기에 대한 경고 및 접근 제한이 되는가?
	향상	자동으로 규정 기준을 적용하고 교정 조치가 가능한가?
		규정 준수에 대한 모니터링 및 이에 따른 접근권한 부여가 가능한가?
	최적화	규정 준수 여부에 따라 동적으로 권한이 수정되는가?
		규정 준수 평가를 AI 기반으로 실시간으로 할 수 있는가?

세부 설명

■ **기존**

✓ **리소스에 연결된 기기를 식별할 수 있는가?**

- 조직 내부 네트워크에 연결된 엔드포인트(PC, 모바일, IoT 등)를 식별하여 할 수 있다. 방화벽, NAC, 등을 통해 IP 주소, MAC 주소 등을 수동으로 수집하거나, 기본적인 에이전트를 통해 정보를 취합한다. 실시간성이 결여되어 정보의 최신성이 낮고, 목록 갱신을 위한 수동 작업이 동반된다.

✓ **수동으로 규정 준수에 대한 확인이 가능한가?**

- 단말 OS 업데이트 여부, 안티바이러스(백신) 설치 여부, 암호화 설정 등 조직이 정의한 기본 보안 정책의 준수 여부를 수동으로 점검한다. 실무 환경에서는 월 1회 '내 PC 지킴이'와 같은 단순 점검 도구를 사용하거나, 보안 점검 체크리스트를 배포하여 사용자가 직접 결과를 제출(자가 점검)하는 방식으로 확인한다. 규정 준수가 실시간으로 강제되지 않고 사후 점검 형태로 이루어진다.

■ **초기**

✓ **실시간으로 기기를 탐지하고 규정 준수를 평가할 수 있는가?**

- EDR, EPP, NAC, UEM 등의 시스템을 바탕으로, 기기가 네트워크에 접속을 시도하는 시점에 실시간으로 탐지한다. 실무 환경에서는 기기의 상태(예시: 백신/보안패치 최신 여부, OS 버전, 필수 S/W 설치 여부 등)를 자동으로 확인하여 사전에 정의된 보안 정책의 규정 준수 여부를 평가한다.

✓ **비준수 기기에 대한 경고 및 접근 제한이 되는가?**

- EDR, EPP, NAC, UEM 등의 시스템을 활용하여 보안 규정이 비준수 된 기기에 대해서는 경고 조치를 취하거나 조직 리소스에 접근을 제한한다. 예를 들어 기기의 상태(OS버전, 필수 S/W 설치 여부 등)를 확인하여 조직 내부 네트워크 접근이 제한된다.

■ **향상**

✓ **자동으로 규정 기준을 적용하고 교정 조치가 가능한가?**

- 비준수 기기에 대해 단순 알림이나 접근 제한을 수행하는 단계를 넘어, 비준수 항목을 능동적으로 교정 조치가 가능하다. 실무 환경에서는 클라이언트 에이전트(EPP, NAC, UEM 등)를 통해 자동으로 누락된 보안 패치를 설치하도록 강제하거나, 원격으로 에이전트을 강제 실행/업데이트하는 등의 자동화된 교정 조치를 수행한다. 또는 웹 기반으로 보안 규정 준수 교정을 강제 유도하여, 사용자가 직접 필수 프로그램을 설치하도록 안내하고 조치가 완료된 이후에만 정상적인 리소스 접근을 허용한다.

✓ **규정 준수에 대한 모니터링 및 이에 따른 접근권한 부여가 가능한가?**

- 기기의 접속 세션이 활성화된 이후에도 기기의 보안 상태 규정 준슈 여부를 지속적으로 모니터링한다. 실무 환경에서는 EDR, EPP, NAC, UEM 등의 에이전트가 기기의 보안 규정 준수 여부(예시: 실시간 백신 동작 여부, 방화벽 활성화 상태, C&C 서버 접속 시도 등)를 실시간으로 감지한다. 이 상태 정보는 정책 엔진(예시: IAM, ICAM, ZTNA 등)과 연동되며, 기기가 비준수 상태로 변경되면 사용자의 시스템 접근권한이 동적으로 조정된다. 예를 들어, 최초 접속 시 '규정 준수' 상태로 '전체 리소스' 접근권한을 부여받았더라도, 세션 중에 '규정 비 준수' 상태가 되면 '제한된 리소스'(예시: 인터넷만 허용, 내부망 차단)만 접근 가능하도록 권한이 실시간으로 하향 조정된다.

■ **최적화**

✓ **규정 준수 여부에 따라 동적으로 권한이 수정되는가?**

- 기기의 규정 준수 상태를 ICAM, ZTNA와 같은 정책 엔진과 실시간으로 연동하여 지속적으로 모니터링 한다. 기기의 상태가 규정 비준수로 판단되면, 정책 엔진이 관리자의 개입 없이 기기의 접근권한을 자동으로 수정하는 등 자동화된 대응을 수행한다. 실무 환경의 예시로는 기기에서 랜섬웨어 감염 징후 등 심각한 비준수 사항이 탐지되는 즉시, SOAR 플레이북 등과 연동된 정책 엔진이 해당 기기의 접근권한을 실시간으로 격리 상태로 동적 수정하여 모든 내부 리소스 접근을 원천 차단한다.

✓ **규정 준수 평가를 AI 기반으로 실시간으로 할 수 있는가?**

- ML/AI 엔진이 기기의 이상 행위, 미확인 프로세스 실행, 실시간 취약 상태 등을 종합적으로 평가한다. 실무 환경에서는 EDR, XDR, ICAM, SIEM/SOAR 등의 시스템을 연계하여 정보를 수집하고, 정적 규칙(예시: 백신 설치 여부 등)만으로는 탐지할 수 없는 실시간 이상 징후를(예시: 평소와 다른 네트워크 트래픽 발생, 권한 상승 시도)를 ML/AI이 실시간으로 분석한다. 이 평가 결과는 기기의 동적인 위험 점수를 실시간으로 스코어링하는 데 사용되며, 이는 리스크 기반의 자동화된 조치로 이어진다.

2.2 데이터 접근제어

항목	2.2.1 실시간 검사를 통한 기기 권한 부여	
설명	기기가 네트워크에 접근하기 전에 보안 상태를 평가(NextGen AV, AppControl, FIM(파일 무결성 모니터링) 등을 이용)하고, 안전한 장치만 접근을 허용하는 기능이다.	
성숙단계	기존	자산 접근 기기에 대한 정보가 수집되는가?
	초기	기기가 자산에 접근하기 전 수동 검사를 수행하는가?
	향상	기기의 상태를 자동으로 평가하고 보안 기준을 충족하는 기기만 접근 허용이 되는가?
	최적화	보안 상태에 따라 기기의 접근권한을 조정할 수 있는가?
		종합적인 기기 보안 전략을 구현하여 다른 보안 시스템과 연동하였는가?

세부 설명

■ **기존**

✓ **자산 접근 기기에 대한 정보가 수집되는가?**

- 조직 리소스에 접근하는 기기에 대한 정보를 수집하기 위한 계획이 수립되고 실행되고 있으며, 실무 환경에서는 기본적인 백신 에이전트나 네트워크 방화벽 수준에서, 조직 네트워크에 접근하는 기기)에 대한 제한적인 정보(예시: IP 주소, 백신 설치 여부 등)가 수집되고 있음을 의미한다. 이 정보는 특정 자산에 대한 접근권한 부여 여부를 판단하는 데 활용될 수 있으나, 수집 정보가 제한적이고 실시간성이 낮다.

■ **초기**

✓ **기기가 자산에 접근하기 전 수동 검사를 수행하는가?**

- 기기가 자산(조직 리소스)에 접근하기 전에 보안 상태를 확인하는 수동 검사 절차를 수행한다. 실무 환경에서는 내PC지킴이, 백신, NAC과 같은 점검 도구를 활용해 검사를 주기적으로(예시: 월 1회 배치 작업) 수행하여, 그 결과를 바탕으로 기기의 보안 상태를 확인한다. 그 결과를 바탕으로 기기의 보안 상태를 확인하고 자산 접근 여부를 판단한다. 이는 자동화된 실시간 검증이 아닌, 정해진 시점에 수동 또는 반자동으로 검사를 수행하는 단계이다.

■ **향상**

✓ **기기의 상태를 자동으로 평가하고 보안 기준을 충족하는 기기만 접근 허용이 되는가?**

- NAC, UEM, EDR 등의 시스템을 바탕으로 실시간으로 기기의 보안 상태(예시: OS 버전, 보안 패치 버전, 백신 실시간 감시 활성화 여부 등)를 자동으로 검사하고, 조직의 보안 기준 준수 여부를 자산 접근 시 지속적으로 평가한다. 이 평가 결과, 보안 기준을 충족하는 기기만 자산 접근을 허용한다.

■ **최적화**

✓ **보안 상태에 따라 기기의 접근권한을 조정할 수 있는가?**

- ML/AI 기반의 실시간 보안 상태 평가를 수행하여 보안 기준 미달 시 시스템 접근을 제한하는 방식으로 기기 권한을 동적으로 조정한다. 실무 환경에서는 기기 단말에서 수집된 동적 정보(예시: 프로세스 실행 내역, 네트워크 트래픽 패턴, 사용자 행위 등)가 ICAM, SIEM/SOAR 등의 시스템과 연동되어 분석된다. ML/AI 엔진은 이 분석 결과를 바탕으로 기기의 동적인 위험 점수를 실시간으로 스코어링 하며, 이 점수가 임계치를 초과할 경우 정책 엔진을 통해 해당 기기의 접근권한을 자동으로 하향 조정하거나 차단하는 등 자동화된 대응을 수행한다.

2.3 자산관리

항목	2.3.1 기기 인벤토리	
설명	모든 기기의 목록을 작성하고 관리하는 시스템이다. 이는 조직의 보안을 위해 모든 장치의 상태, 소유자, 위치 등을 정확히 파악할 수 있게 해준다. 기기 속성에는 PKI(802.1x) 시스템 인증서, 기기 개체, 패치/취약성 상태 등을 확인할 수 있는 기술 세부 정보가 포함된다.	
성숙단계	기존	기기의 인벤토리를 작성하고 수동으로 업데이트하는가?
		주요 기기에 대한 정보를 수집하고 관리하는가?
	초기	기기 인벤토리를 자동화하고 모든 기기를 실시간으로 기록하는가?
	향상	기기 인벤토리에 비정상적이거나 승인되지 않은 기기를 탐지하는 기능을 포함하는가?
		인벤토리 분석을 통하여 보안 취약점을 파악하는가?
	최적화	실시간 모니터링 및 이상 행위 예측 분석을 통해 기기 관리를 수행하는가?

세부 설명

■ **기존**

✓ **기기의 인벤토리를 작성하고 수동으로 업데이트 하는가?**

- 조직 내에서 사용하는 기기를 목록화하기 시작하는 단계로, 조직 내 기기 도입 시 특정 문서 파일이나 스프레드시트 등을 활용해 자산관리대장을 수작업으로 관리하며, IP주소, MAC 주소, 기기명, 담당자 정도만 관리된다. 기기 상태나 보안 정보는 포함되지 않으며, 실시간성이나 정확성은 낮은 편이다.

✓ **주요 기기에 대한 정보를 수집하고 관리하는가?**

- 서버, 업무용 데스크탑 등 주요 기기에 한정하여 자산 정보를 수집한다. 실무 환경에서는 단순 에이전트(백신, EPP, NAC 등) 기반으로 제한된 정보를 수집하거나, 관리자가 수동 조사를 통해 정보를 취합하여 자산관리대장(스프레드시트 등)에 반영한다. 이 단계에서는 전체 기기를 포괄하지 못하며, 수집되는 정보 항목(IP, MAC, 관리자명 등)도 한정적인 경우가 많다.

■ **초기**

✓ **기기 인벤토리를 자동화하고 모든 기기를 실시간으로 기록하는가?**

- 문서 기반의 자산관리대장에서 벗어나 ITAM 시스템 등을 통해 기기의 구매, 배포, 폐기 등 기본적인 라이프사이클 정보를 관리하기 시작한다. Directory, EPP, NAC 등의 시스템을 통해 조직 내부 리소스에 연결된 기기를 탐지하고 식별하여 인벤토리를 관리할 수 있다. 이 단계에서는 운영체제, 패치 상태, 위치 정보, 사용자 연계 정보 등 기기의 정보들을 확인하고 인벤토리를 관리할 수 있으나, 조직 내부 자산으로 등록되지 않은 개인 기기나 IoT 기기에 대한 식별은 일부 제한될 수 있다.

■ **향상**

✓ **기기 인벤토리에 비정상적이거나 승인되지 않은 기기를 탐지하는 기능을 포함하는가?**

- 네트워크에 새로운 기기 접근 시 인벤토리를 실시간으로 업데이트하며, 기 등록된 MAC 주소, 인증서, 사용자 속성 등의 정보를 바탕으로 비정상적이거나 승인되지 않은 기기인지를 판단한다. 실무 환경에서는 EDR, ZTNA, NDR 시스템 등을 통해 실시간으로 기기의 보안 상태를 확인하고, 승인되지 않은 기기가 조직 내 리소스에 접근하는 것을 탐지하여 대응할 수 있다. SIEM/SOAR와 연동하여 기기 인벤토리에 대한 시나리오와 플레이북을 통해 이상 기기에 대한 내용을 관리자에 경고 알림을 보내고 즉각적인 대응을 수행한다.

✓ **인벤토리 분석을 통하여 보안 취약점을 파악하는가?**

- 수집된 기기 속성 데이터(OS 버전, 패치 상태, 네트워크 연결 정보 등)를 기반으로 보안 취약점을 식별하고 대응한다. 실무 환경에서는 EDR, ZTNA, NDR, XDR 시스템 등을 통해 기기의 보안 취약점(예시: 패치 미적용, 구형 OS 사용, 승인되지 않은 앱 실행 등)을 탐지하고, 필요한 경우 차단 등의 대응 조치를 수행한다. 또한, 이러한 보안 시스템과 ITAM 시스템을 연동하여 탐지된 취약점 정보나 상태 변경 사항을 기기 인벤토리에 실시간으로 업데이트 및 관리할 수 있다.

■ **최적화**

✓ **실시간 모니터링 및 이상 행위 예측 분석을 통해 기기 관리를 수행하는가?**

- ML/AI 기반 인벤토리 관리 플랫폼을 바탕으로 기기의 행동 패턴, 소프트웨어 설치 변화, 네트워크 활동 정보 등을 분석하여 기기 위험도를 실시간으로 판단한다. 실무 환경에서는 기기의 과거 데이터와 현재 상태를 ML/AI 엔진이 지속적으로 분석하여, 단순 이상 행위 탐지를 넘어 향후 발생 가능한 위험(예시: 특정 S/W 설치 후 악성 행위 발생 가능성 예측)을 예측 분석한다. 이 분석 결과는 SIEM/SOAR 및 ICAM/ZTNA와 같은 정책 엔진과 연동되어, 예측된 위험이나 실제 기기 이상 행위 탐지 시 관리자 알림뿐만 아니라 해당 기기의 접근권한을 자동으로 제한하거나 격리하는 등의 선제적이고 자동화된 기기 관리 및 대응 조치를 수행한다.

항목	2.3.2 통합 엔드포인트 관리 및 모바일 기기 관리	
설명	모든 엔드포인트와 모바일 기기를 중앙에서 통합 관리하고, 보안을 유지하는 기능이다. 이는 원격으로 관리될 수 있어야 하며, 보안 정책을 적용할 수 있어야 한다.	
성숙단계	기존	기본적인 엔드포인트 및 모바일 기기 관리 시스템이 도입되었는가?
		기본적인 보안 정책을 설정하였는가?
	초기	엔드포인트 및 모바일 기기의 보안 설정을 중앙에서 관리하고 보안 업데이트를 자동 배포하는가?
		기기 상태를 지속적으로 모니터링 하는가?
	향상	모든 엔드포인트와 모바일 기기에 대하여 보안 정책을 중앙에서 자동으로 적용하고 관리하는가?
	최적화	모든 기기의 보안을 중앙에서 통합적으로 관리하고, 자동화된 위협 대응이 가능한가?

세부 설명

■ **기존**

✓ **기본적인 엔드포인트 및 모바일 기기 관리 시스템이 도입되었는가?**

- 엔드포인트 및 모바일 기기 관리가 시작되는 단계로, 주로 MDM 솔루션이 도입되어 운영된다. MDM은 IT 부서가 직원 소유 또는 기업 소유의 스마트폰, 태블릿 등 모바일 기기를 원격으로 등록하고 추적하며 기본적인 관리 및 보호 기능을 수행하는 데 중점을 둔다. 실무 환경에서는 MDM 외에도 NAC, 무선 AP, 방화벽 등의 시스템을 통해 조직 리소스에 접근하는 엔드포인트나 모바일 기기를 제한적으로 식별할 수 있다.

✓ **기본적인 보안 정책을 설정하였는가?**

- 암호 설정, 원격 잠금, 초기화 등의 단순 보안 정책을 설정하고 수동 또는 제한적으로 적용한다. 중앙집중화된 관리는 수행되지 않으며, 주로 수동으로 정책 준수를 확인한다. 실무 환경에서는 모바일 기기나 태블릿으로 접근할 수 있는 업무 영역(예시: 이메일, 그룹웨어)을 정책적으로 정의하고, MDM과 같은 통합 관리 솔루션이 설치되지 않은 기기라도 모바일 앱 자체의 보안 기능(예시: 앱 내 데이터 접근권한 관리, 화면 캡처 방지)을 활용하여 기본적인 보안 조치를 적용하는 수준을 의미한다. 엔드포인트 보안 정책을 수립할 때에는 관리 범위를 기존의 PC, 모바일 기기뿐만 아니라 IoT 기기(스마트 워치, 프린터 등)와 OT 장비까지 확장하기 위한 보안 조치 및 통합관리 방안을 고려한다.

■ **초기**

✓ **엔드포인트 및 모바일 기기의 보안 설정을 중앙에서 관리하고 보안 업데이트를 자동 배포하는가?**

- 통합 모바일 기기 관리 시스템(MDM, MAM 등)을 바탕으로 엔드포인트 및 모바일 기기의 보안 설정을 중앙에서 관리한다. 실무 환경에서는 관리 콘솔을 통해 암호화 설정, 패치 적용 등 보안 설정을 일괄적으로 적용하며, 일정에 따라 보안 업데이트가 자동으로 배포되기 시작한다.

✓ **기기 상태를 지속적으로 모니터링 하는가?**

- 각 엔드포인트에 설치치된 보안 에이전트(EDR, MDM 등) 또는 네트워크 스캐닝 등을 통해 기기의 상태(OS 버전, 보안 패치 적용 여부, 기본 보안 설정 준수 여부 등)를 주기적으로 수집하고 이상 여부를 모니터링한다. 관리 범위에 포함된 다양한 종류의 기기(PC, 모바일, IoT, OT 등)에 대한 상태 정보를 수집하고 관리 시스템 대시보드를 통해 현황을 확인한다.

■ **향상**

✓ **모든 엔드포인트와 모바일 기기에 대하여 보안 정책을 중앙에서 자동으로 적용하고 관리하는가?**

- 사용자, 부서, 기기 그룹에 따른 정책 템플릿을 설정한 후 통합 관리 시스템(UEM, ITAM 등)을 통해 각 그룹에 적합한 정책을 자동적으로 적용한다. EDR, XDR 등의 탐지 솔루션과 연계하여 각 기기의 정책 준수 여부를 실시간으로 모니터링하며, 보안 이벤트 발생 시 관리자에게 알림을 보내고 자동으로 조치를 수행한다.

■ **최적화**

✓ **모든 기기의 보안을 중앙에서 통합적으로 관리하고, 자동화된 위협 대응이 가능한가?**

- ML/AI 기반의 단일화된 엔드포인트 통합 관리 플랫폼에서 전사 모든 엔드포인트 관리를 수행한다. 실무 환경에서는 기기 유형별로 최적화된 관리 시스템(예: PC/노트북은 EDR, 모바일/프린터는 UEM, 모니터 등 기타 자산은 XDR, ITAM 등)에서 수집된 정보가 단일 플랫폼으로 통합된다. 이 통합 플랫폼을 통해 정책 변경이나 패치 발생 시 해당하는 모든 기기에 자동으로 적용하며, ML/AI이 학습한 기기 사용 패턴을 바탕으로 비정상 행동을 탐지되면 ICAM, ZTNA 등의 시스템과 연동하여 해당 기기를 격리시키거나 접근권한을 제한하는 등의 자동화된 위협 대응을 실시간으로 수행한다.

2.4 기기 위협 보호

항목	2.4.1 엔드포인트 및 확장된 탐지·대응(EDR 및 XDR)	
설명	엔드포인트와 확장된 영역에서 실시간으로 위협을 탐지하고 대응하는 고급 보안 솔루션으로 이를 이용하여 엔드포인트의 이상행위를 탐지해야 한다.	
성숙단계	기존	기본적인 EDR 솔루션을 도입하였는가?
	초기	EDR 시스템을 고도화하여 실시간 위협 탐지 및 자동 대응이 가능한가?
	향상	XDR 솔루션을 도입하였는가?
	최적화	AI 기반 EDR·XDR 솔루션을 통해 실시간으로 모든 기기에 대한 위협 탐지가 가능한가?

세부 설명

■ **기존**

✓ **기본적인 EDR 솔루션을 도입하였는가?**

- 위협에 대한 탐지/차단 정책을 수립하고 EDR 솔루션을 도입하여 기본적인 멀웨어, 악성 프로세스, 파일 변경 등의 위협을 탐지한다. 실무 환경에서는 엔드포인트에서 발생하는 위협 행위를 EDR 콘솔을 통해 확인하는 수준이며, 발견된 위협에 대해서는 주로 관리자가 수동으로 분석하고 대응 조치를 수행한다.

■ **초기**

✓ **EDR 시스템을 고도화하여 실시간 위협 탐지 및 자동 대응이 가능한가?**

- EDR 시스템을 고도화하여 실시간 모니터링, 자동 차단, 격리, 경로 추적 등의 보안 기능을 수행한다. 발견된 위협에 대해 즉각적으로 기기를 차단하거나 파일을 삭제하는 등의 자동화된 대응을 수행한다. 실무 환경에서는 EDR 전담 담당자를 배정하여 엔드포인트 위협을 지속적으로 모니터링하고 탐지 정책을 강화하거나, 외부 MDR 서비스를 활용하여 엔드포인트에 대한 실시간 대응 체계를 구현할 수 있다.

■ **향상**

✓ **XDR 솔루션을 도입하였는가?**

- EDR의 탐지 범위에서 확장되어 넘어 네트워크, 서버, 클라우드, 이메일 등의 위협을 탐지하고 대응하는 XDR 시스템을 도입한 단계이다. 실무 환경에서는 엔드포인트에서 발생한 이벤트와 네트워크 트래픽 정보, 클라우드 접근 로그 등을 상관관계 분석하여, 개별 EDR만으로는 파악하기 어려운 복합적인 공격 흐름(예시: 이메일을 통한 악성코드 유입 → 엔드포인트 감염 → 내부망 확산 시도)을 하나의 통합된 공격으로 인식하고 추적하여 대응할 수 있다. 또한, 머신러닝(ML) 기반의 자동 분석 엔진을 바탕으로 위협 탐지 정확도를 향상시키며, 학습한 정상 행위 패턴을 기반으로 이상 행위를 탐지한다.

■ **최적화**

✓ **AI 기반 EDR·XDR 솔루션을 통해 실시간으로 모든 기기에 대한 위협 탐지가 가능한가?**

- ML/AI 기반의 이상 행위 탐지 엔진이 전사 모든 엔드포인트를 실시간으로 분석하고, 위협이 발생하면 해당 기기를 격리하거나 접근권한을 제한하는 등의 자동화된 조치를 수행한다. 실무 환경에서는 외부의 위협 인텔리전스(TI) 정보와 연동하여 최신 IOC(침해 지표)/IOA(공격 지표) 정보, 공격 캠페인 정보 등의 위협 정보를 EDR/XDR 시스템에 실시간으로 반영한다. 이를 통해 알려지지 않은 위협까지 탐지하고, 분석된 위협 정보를 바탕으로 리스크를 예측하여 선제적인 방어 체계를 수립하는 등 자동화된 대응 전략을 수행한다.

항목	2.4.2 자산, 취약성 및 패치 관리 자동화	
설명	네트워크에 연결된 모든 장치의 보안 취약점을 관리하고, 최신 보안 패치를 자동으로 적용하는 기능이다.	
성숙단계	기존	자산 및 취약성을 수동으로 평가하는가?
		주요 자산 및 취약성 목록이 작성되어 있는가?
	초기	자동화된 취약성 평가 및 패치 관리 도구를 도입하여 취약성 발견 시 자동 패치가 이루어지는가?
	향상	모든 자산에 대해 지속적인 취약성 평가 및 패치 관리가 자동화되어 있는가?
		취약성 및 패치 관리 시스템을 다른 보안 시스템과 통합하여 종합적인 보안 관리가 가능한가?
	최적화	취약점을 사전에 식별하고 자동으로 패치 적용이 가능한가?
		자산관리, 취약성 평가, 패치 관리 시스템이 통합되어 있는가?

세부 설명

■ **기존**

✓ **자산 및 취약성을 수동으로 평가하는가?**

- 조직 내 네트워크에 연결된 기기 및 소프트웨어 자산에 대한 목록을 작성하고, 필요한 자산에 대해서 보안 담당자가 수동으로 주기적(예시: 월 1회 / 연 1회) 또는 필요 시 취약점 진단 도구를 사용하여 취약성 점검을 수행한다. 실무 환경에서는 자산 목록과 취약점 점검 결과가 별도로 관리되며, 실시간 연동이나 자동화된 평가는 이루어지지 않는다.

✓ **주요 자산 및 취약성 목록이 작성되어 있는가?**

- 주요 자산과 알려진 취약점(예시: CVE 목록)을 취약점 관리 문서 등을 통해 관리하는 단계이다. 실무 환경에서는 이 목록이 정기적으로 갱신되지 않아 최신 상태가 아니거나, 모든 자산과 취약점을 포괄하지 못하는 경우가 많다. 따라서 취약점 정보의 실시간성이나 정확성은 낮은 편이다.

■ **초기**

✓ **자동화된 취약성 평가 및 패치 관리 도구를 도입하여 취약성 발견 시 자동 패치가 이루어지는가?**

- 취약성 관리 시스템이나 PMS 시스템을 통해 자동화된 취약성 탐지 및 패치 배포 프로세스를 구현하기 시작하는 단계이다. 실무 환경에서는 이러한 전용 시스템 이외에도 EPP, EDR의 취약점 탐지 기능, 또는 Directory의 그룹 정책(GPO)을 통한 패치 배포 기능 등을 활용할 수 있다. 주기적으로(예: 월 1회, 주 1회) 자산을 스캔하여 알려진 취약점을 탐지하고, 패치 관리 시스템이나 Directory 등을 통해 관련 패치를 자동으로 배포하는 기능이 적용된다. 다만, 이 단계에서는 자동 패치 적용 범위가 일부 시스템에 한정되거나, 중요도에 따라 관리자 승인 후 배포되는 등 완전 자동화로 가기 위한 초기 수준을 의미한다.

■ **향상**

✓ **모든 자산에 대해 지속적인 취약성 평가 및 패치 관리가 자동화되어 있는가?**

- 정의된 취약점 관리 프로세스에 따라 온프레미스, 클라우드, 모바일 등 모든 IT 자산에 대한 취약점 진단을 지속적으로(예시: 상시 또는 일 단위) 수행하고 필요 시 자동으로 패치를 수행한다. 실무 환경에서는 취약점 관리 시스템, EPP, EDR 등에서 취약점 평가를 수행하고, 발견된 취약점은 위험도 및 자산 중요도에 따라 분류된다. 분류 결과에 따라 Directory, PMS, EPP, EDR 등을 통해 패치 배포가 자동화되거나 승인 후 배포되는 취약점 조치 워크플로우를 운영한다.

✓ **취약성 및 패치 관리 시스템을 다른 보안 시스템과 통합하여 종합적인 보안 관리가 가능한가?**

- 중앙 관리 시스템(정보보안 포털, ICAM 등)을 통해 Directory, ITAM, EPP, EDR 등의 보안 시스템과 연동하여 중앙집중화된 취약점 및 패치 관리를 수행한다. 실무 환경에서는 각 시스템 영역에서 수행된 취약점 관리 프로세스(평가, 분류, 조치) 결과가 중앙 관리 시스템으로 통합되어 가시화된다. 또한, 취약점 발견 시 해당 정보가 SIEM으로 전송되어 위협 인텔리전스와 연계 분석되거나, SOAR 플레이북을 통해 자동으로 대응 조치(예시: EDR을 통한 임시 차단 정책 적용, EPP/PMS를 통한 자동화된 OS 패치 등)가 수행되는 등 종합적인 보안 관리 및 자동화된 조치가 이루어진다.

■ **최적화**

✓ **취약점을 사전에 식별하고 자동으로 패치 적용이 가능한가?**

- ML/AI를 기반으로 기 등록된 자산의 속성 정보(설치된 S/W, 구성 설정 등)를 학습하여 이상 행위를 탐지하고, 외부 위협 인텔리전스(TI)를 통합하여 알려지지 않은 취약점(Zero-Day 등)까지 사전에 식별하고 예측한다. 식별된 취약점은 위험도, 자산 중요도, 비즈니스 영향도 등을 고려하여 패치 우선순위가 자동으로 지정되고 자동화된 패치 배포가 이루어진다. 실무 환경에서는 최신 위협 동향과 자산의 행위 분석 결과를 통합하여, 단순히 알려진 취약점에 대응하는 것을 넘어 보다 지능적이고 선제적인 보안 유지가 가능해진다.

✓ **자산관리, 취약성 평가, 패치 관리 시스템이 통합되어 있는가?**

- 자산 인벤토리, 취약성 평가, 패치 관리가 단일 플랫폼 또는 통합 대시보드로 완벽하게 연계되어 실시간으로 현황을 파악하고 정책을 집행한다. 실무 환경에서는 ITAM, EDR/XDR, EPP/PMS 등 개별 시스템의 정보가 정보보안 포털이나 ICAM 시스템 등으로 집약되어, 관리자가 한 곳에서 모든 자산의 취약점 상태를 확인하고 필요한 패치 조치를 승인하거나 자동화 정책을 설정할 수 있다.

3. 네트워크

3.1 네트워크 세분화

항목	3.1.1 매크로 세그멘테이션	
설명	매크로 세그멘테이션은 네트워크를 대규모 세그먼트로 나누어 주요 보안 영역을 구분하는 기술이다. 이는 네트워크 전체를 보호하는데 필요한 보안 경계를 설정하는데 사용된다.	
성숙단계	기존	비즈니스 영역별로 매크로 세그멘테이션이 되어 있는가?
		네트워크 내 주요 자산과 트래픽 흐름 기반으로 매크로 세그먼트가 구성되어 있는가?
	초기	매크로 세그먼트 간에 보안 정책을 적용하였는가?
		매크로 세그먼트 간에 트래픽을 모니터링하고 비정상적 활동을 탐지하는가?
	향상	매크로 세그먼트 간 맞춤형 보안 정책이 설정되었는가?
		매크로 세그먼트 간 트래픽을 조정하고 보안 위협에 대응 가능한가?
	최적화	AI 기반 매크로 세그먼트 관리 도구가 적용되었는가?

세부 설명

■ **기존**

✓ **비즈니스 영역별로 매크로 세그멘테이션이 되어 있는가?**

- 조직 내부의 네트워크가 목적에 맞게 논리적 또는 물리적으로 분리된다. 실무 환경에서는 인터넷망, 업무망, 개발망 등과 같이 큰 단위의 비즈니스 영역별로 네트워크를 구분하는 것을 의미한다. VLAN, 서브넷, 라우팅 기술들이 적용되어 있으며, 주로 방화벽을 통해 각 세그먼트 간의 기본적인 접근제어가 이루어진다.

✓ **네트워크 내 주요 자산과 트래픽 흐름 기반으로 매크로 세그먼트가 구성되어 있는가?**

- 시스템(서버), 데이터베이스, 핵심 애플리케이션 등 주요 자산을 중심으로, 네트워크 목적에 맞게 트래픽 흐름을 분석하고 기능 단위의 세그먼트를 구성하기 시작한다. 실무 환경에서는 주요 망간(예시: 업무망 ↔ 인터넷망 등)의 네트워크 트래픽 흐름을 수동으로 분석하여 세그멘테이션의 기준을 수립하고 필요한 보안 정책(예시: 특정 포트 허용/차단 등)을 정의하는 단계를 의미한다.

■ **초기**

✓ **매크로 세그먼트 간에 보안 정책을 적용하였는가?**

- 각 세그먼트 간 트래픽에 대해 ACL, 방화벽 정책 등을 통해 인바운드/아웃바운드 트래픽 제어를 수행한다. L3 방화벽 등이 각 세그먼트 경계에 위치하며, 세그먼트 간 통신은 정의된 정책 및 최소

권한 원칙을 기반으로 통제된다. 실무 환경에서는 망연계 시스템이나 VDI 시스템 등을 활용하여 특정 경로(예시: 인터넷망 → 업무망 등)의 파일 전송이나 서비스 접근을 제어하고 결재 프로세스 등을 적용할 수 있다.

✓ **매크로 세그먼트 간에 트래픽을 모니터링하고 비정상적 활동을 탐지하는가?**

- 각 세그먼트 간의 트래픽을 모니터링하여 비정상적인 활동(예시: 내부 자료의 비정상적인 대량 전송 시도, 허용되지 않은 세그먼트 간 접근 우회 시도 등)을 탐지하기 시작한다. 실무 환경에서는 방화벽 로그, 네트워크 트래픽 분석 도구(예시: NetFlow, sFlow 등) 등을 활용하여 기본적인 트래픽 패턴을 분석하고, 사전에 정의된 임계치를 초과하거나 정책 위반 시도가 발생하면 관리자에게 경고를 보낸다.

■ **향상**

✓ **매크로 세그먼트 간 맞춤형 보안 정책이 설정되었는가?**

- 각 매크로 세그먼트의 기능, 리스크 수준, 자산 민감도에 따라 세분화된 맞춤형 보안 정책을 적용한다. 실무 환경에서는 SDN 기술 등을 활용하여, 중앙 정책 엔진에서 각 세그먼트별 특성을 고려한 보안 정책을 동적으로 관리하고 적용한다. 예를 들어, 민감 데이터가 포함된 세그먼트에는 더 엄격한 접근제어 규칙을 적용하고, 일반 업무 세그먼트에는 상대적으로 완화된 정책을 적용하는 등 차등화된 관리가 가능하다.

✓ **매크로 세그먼트 간 트래픽을 조정하고 보안 위협에 대응 가능한가?**

- SDN 컨트롤러 등을 기반으로 네트워크 트래픽 흐름을 프로그래밍 방식으로 제어하며, 보안 위협에 동적으로 대응한다. 실무 환경에서는 SIEM/SOAR 등 보안 시스템과 연동하여, 특정 세그먼트에서 이상 트래픽이나 보안 위협이 탐지될 경우 SDN 컨트롤러가 해당 세그먼트의 트래픽을 조정하거나 네트워크에서 격리하는 등의 동적 조치를 수행할 수 있다.

■ **최적화**

✓ **AI 기반 매크로 세그먼트 관리 도구가 적용되었는가?**

- ML/AI를 기반으로 세그먼트 간 통신 패턴을 학습하여 정상 행위 기준선을 설정하고, 이를 벗어나는 비정상 연결이나 위협을 예측하고 식별한다. 실무 환경에서는 SDN, ZTNA, ICAM, SIEM/SOAR 등의 시스템과 연동하여, AI가 위협을 예측하거나 감지하면 정책 기반의 자동화된 조치를 실시간으로 수행한다. 예를 들어, AI가 특정 세그먼트의 감염 위험을 예측하면, 자동으로 해당 세그먼트를 네트워크에서 격리시키거나 주요 자산을 안전한 세그먼트로 재배치하는 등 자율적인 관리 및 대응이 이루어진다.

항목	3.1.2 마이크로 세그멘테이션	
설명	마이크로 세그멘테이션은 네트워크를 세분화하여 각 워크로드나 애플리케이션별로 세그먼트를 설정하는 기술로, 보다 정밀한 보안 제어를 가능하게 한다. 접속하는 ID 또는 응용 접근을 기반으로 네트워크 세분화를 정의하거나 물리적 세분화를 수행하고 문서화하여야 한다. 또한 가능하다면 호스트 수준의 프로세스 마이크로 세그멘테이션을 수행한다.	
성숙단계	기존	애플리케이션 및 워크로드 기준으로 마이크로 세그멘테이션이 되어 있는가?
		수동으로 세그먼트를 구성하는가?
	초기	애플리케이션 및 워크로드에 따른 마이크로 세그멘테이션 보안 정책이 설정되었는가?
		네트워크 수준에서 마이크로 세그멘테이션을 수행하여 워크로드 간 이동을 탐지·차단할 수 있는가?
		마이크로 세그먼트 간 트래픽 모니터링이 가능한가?
	향상	모든 네트워크 트래픽에 대한 보안 정책 설정 및 제어가 가능한가?
		애플리케이션별 격리 메커니즘이 적용되었는가?
	최적화	AI 기반 마이크로 세그먼트 관리 도구가 적용되어 위협에 자동으로 대응 가능한가?

세부 설명

■ **기존**

✓ **애플리케이션 및 워크로드 기준으로 마이크로 세그멘테이션이 되어 있는가?**

- 애플리케이션, 워크로드 단위로 기본적인 트래픽 분리를 수행하며, 각 단위에 수동으로 보안 정책을 적용 한다. 실무 환경에서는 웹 서버, DB 서버 등 시스템 내의 애플리케이션 단위로 네트워크 세그먼트를 나눌 수 있다. 정책은 주로 방화벽 또는 ACL을 활용한 정적인 형태로 구성된다.

✓ **수동으로 세그먼트를 구성하는가?**

- 관리자가 네트워크 흐름을 분석하고 수동으로 각 세그먼트를 정의하며, 세그먼트별 정책 설정 또한 수동으로 수행된다. 실무 환경에서는 새로운 애플리케이션이나 워크로드가 추가될 때마다 관리자가 직접 네트워크 장비(방화벽, 라우터 등) 기준으로 세그먼트 및 정책을 설정/변경해야 함을 의미한다.

■ **초기**

✓ **애플리케이션 및 워크로드에 따른 마이크로 세그멘테이션 보안 정책이 설정되었는가?**

- 각 애플리케이션 및 워크로드 별로 독립된 세그먼트 구성을 부분적으로 자동화하거나 중앙 관리 도구를 통해 효율적으로 맞춤형 보안 정책을 적용한다. 실무 환경에서는 접속하는 ID 또는 애플리케이션 접근을 기반으로 네트워크 세분화를 정의하거나 물리적 세분화를 수행하고 문서화한다. 보안 정책은 중앙 정책 엔진 등을 통해 관리될 수 있다.

✓ **네트워크 수준에서 마이크로 세그멘테이션을 수행하여 워크로드 간 이동을 탐지·차단 할 수 있는가?**

- 워크로드 간 트래픽 흐름을 L4/L7 수준으로 식별하고, 허용되지 않은 트래픽 흐름(예시: 비인가된 워크로드 간 통신 시도 등)을 탐지하고 차단한다. 실무 환경에서는 호스트 기반 방화벽이나 네트워크 방화벽, IPS 등을 활용하여 정의된 정책에 따라 워크로드 간 이동을 제어한다.

✓ **마이크로 세그먼트 간 트래픽 모니터링이 가능한가?**

- 각 마이크로 세그먼트 간의 트래픽 흐름을 실시간으로 수집하고, 기본적인 네트워크 관리 시스템(NMS) 수준 이상의 분석을 수행한다. 실무 환경에서는 수집된 트래픽 로그를 SIEM 등의 보안 분석 시스템과 연계하여 비정상적인 통신 시도나 정책 위반 여부를 확인하고 관리자에게 경고를 보낸다. 이 단계에서는 주로 사전에 정의된 규칙 기반으로 이상 징후를 탐지한다.

■ **향상**

✓ **모든 네트워크 트래픽에 대한 보안 정책 설정 및 제어가 가능한가?**

- 클라우드 기반 컨테이너, VM 등의 동적 자산을 포함하여 모든 네트워크 트래픽에 대한 정책을 설정한다. 실무 환경에서는 NDR 등을 통해 풀 패킷 기반의 트래픽 가시성을 확보하고, ZTNA 또는 NGFW 등의 시스템을 활용하여 단순 포트 기반이 아닌 특정 애플리케이션, 프로세스, 사용자 ID 등의 트래픽 흐름을 식별하여 보안 정책을 설정하고 상세 세그먼트 단위의 제어를 수행한다.

✓ **애플리케이션 별 격리 메커니즘이 적용되었는가?**

- 애플리케이션 별로 사용자/ID, 리스크 수준을 기반으로 하는 격리 메커니즘을 적용하여 컨테이너, 호스트 단위의 세그먼트를 수행한다. 실무 환경에서는 호스트 기반 마이크로 세그멘테이션 시스템이나 개별 호스트 방화벽 체계를 통합 관리하여, 워크로드 내부의 프로세스 수준까지 통신을 제어하고, 허가되지 않은 통신을 차단하는 등 정교한 격리 정책을 적용한다.

■ **최적화**

✓ **AI 기반 마이크로 세그먼트 관리 도구가 적용되어 위협에 자동으로 대응 가능한가?**

- ML/AI 분석 엔진이 지속적인 네트워크 트래픽 모니터링을 통해 네트워크 및 워크로드 트래픽을 실시간으로 분석하여 정상/비정상 트래픽을 식별하고, AI 기반으로 최신화된 네트워크 토폴로지 맵을 관리한다. 실무 환경에서는 호스트 기반 마이크로 세그멘테이션 시스템이나 SIEM/SOAR, ZTNA 등 제어 시스템과 연동하여 비정상 트래픽이나 위협이 식별되면 자동으로 보안 정책을 조정하거나 세그먼트별 개별 방화벽 정책을 생성 및 반영하여 워크로드를 격리하는 등의 자동화된 조치를 수행한다. 이를 통해 내부 자산들에 대한 개별 방화벽 체계를 통해 '횡적 이동(Lateral Movement)' 자체를 효과적으로 차단한다.

항목	3.1.3 소프트웨어 정의 네트워킹	
설명	네트워크를 소프트웨어 기반으로 관리하고 제어하는 기술로, SDN 프로그래밍 가능 인프라를 구현하여 제어 영역과 데이터 영역을 분리하고 데이터 영역의 요소를 중앙에서 관리 및 제어를 수행한다. 네트워크 유연성을 높이고 보안을 강화하는데 사용된다.	
성숙단계	기존	소프트웨어 정의 네트워크가 도입되어 있는가?
		클라우드 적용 시, SDN 기본 구조를 설정하고 트래픽을 제어할 수 있는가?
	초기	클라우드 적용 시, SDN을 활용하여 네트워크 트래픽을 중앙에서 관리하고, 정책을 실시간으로 적용 가능한가?
	향상	클라우드 적용 시, SDN 기능을 확장하여 트래픽 관리 및 보안을 적용하고 있는가?
	최적화	클라우드 적용 시, AI 기반 위협 관리 및 트래픽 예측 등이 가능한 SDN 기능을 적용하였는가?

세부 설명

■ **기존**

✓ **소프트웨어 정의 네트워크가 도입되어 있는가?**

- SDN 컨트롤러 기반의 네트워크 인프라 구성이 시작되는 단계이다. 네트워크 장비의 제어 영역(Control Plane)과 데이터 영역(Data Plane)을 분리하여, 중앙 컨트롤러를 통해 네트워크 정책 및 트래픽 경로를 관리하는 기본적인 SDN 구조를 도입한다.

✓ **클라우드 적용 시, SDN 기본 구조를 설정하고 트래픽을 제어할 수 있는가?**

- 하이브리드 또는 클라우드 환경에 SDN 구조를 설정하여 네트워크 경로를 정의한다. 실무 환경에서는 SDN 컨트롤러를 기반으로 데이터 영역 내의 네트워크 트래픽을 제어하여 중앙 집중화된 관리를 시작하는 단계를 의미한다.

■ **초기**

✓ **클라우드 적용 시, SDN을 활용하여 네트워크 트래픽을 중앙에서 관리하고, 정책을 실시간으로 적용 가능한가?**

- 중앙 집중식 SDN 컨트롤러를 통해 클라우드 환경의 트래픽 흐름을 모니터링하기 시작하며, 네트워크 QoS, 접근제어, 우회 경로 설정 등을 정책 기반으로 실시간 적용하는 단계이다. 실무 환경에서는 온프레미스에서 사용하던 네트워크 보안 정책(예시: 특정 IP 대역 차단)을 SDN 환경에 통합하여 적용함으로써 하이브리드 환경에 일관된 보안 정책을 반영할 수 있다.

■ **향상**

✓ **클라우드 적용 시, SDN 기능을 확장하여 트래픽 관리 및 보안을 적용하고 있는가?**

- 클라우드 워크로드 간 세그먼트를 세분화하여 SDN 컨트롤러를 통한 세밀한 제어를 수행한다. 실무 환경에서는 AWS, Azure, NCP 등 퍼블릭 클라우드의 VPC(Virtual Private Cloud) 환경에서 제공하는

SDN 기능을 활용하여 가상 네트워크 내 트래픽 관리 및 보안 기능을 확장 적용한다. SDN은 조직의 보안 정책 프레임워크와 통합되어, 단순히 트래픽 경로를 제어하는 것을 넘어 내부의 ICAM, NDR, SIEM/SOAR, ZTNA, 마이크로 세그멘테이션 시스템 등과 연동하여 세그먼트별 보안 정책을 실시간으로 자동 적용하고 네트워크 성능을 최적화한다.

■ **최적화**

✓ **클라우드 적용 시, AI 기반 위협 관리 및 트래픽 예측 등이 가능한 SDN 기능을 적용하였는가?**

- ML/AI 기반의 SDN 관리 시스템을 바탕으로 트래픽 패턴을 학습하여 트래픽 혼잡을 예측하거나 이상 트래픽을 탐지한다. 실무 환경에서는 SDN 컨트롤러가 ICAM, NDR, SIEM/SOAR, ZTNA, 마이크로 세그멘테이션 시스템 등과 연동하여, ML/AI 엔진이 식별한 예측 정보나 탐지된 이상 징후에 따라 자동으로 보안 정책을 조정하거나 네트워크 세그먼트를 동적으로 변경/격리하는 등의 자율적인 조치를 수행한다. 이는 실시간 위협 관리 및 선제적인 네트워크 성능 최적화를 가능하게 한다.

3.2 위협 대응

항목	3.2.1 위협 대응	
설명	위협 대응 기능은 네트워크 내에서 발생하는 모든 잠재적 위협을 신속하게 감지하고 대응하는 시스템을 말한다. 이 기능은 침입 탐지 및 방지 시스템(IDS/IPS), 위협 인텔리전스, 자동화된 대응 시스템 등을 포함한다.	
성숙단계	기존	IDS·IPS 등의 솔루션을 도입하여 주요 위협에 대한 감시 체계가 이루어지고 있는가?
		네트워크 정적 규칙에 의한 수동적 트래픽 관리가 이루어지는가?
	초기	자동화된 위협 탐지 및 대응 시스템이 도입되어 보안 이벤트 발생 시 즉각 대응이 가능한가?
		애플리케이션 프로파일에 따른 트래픽 관리가 이루어지는가?
	향상	실시간 위협 탐지 및 위협 행위에 대한 선제적 대응 체계가 마련되어 있는가?
		네트워크 동적 규칙에 의한 네트워크 트래픽 관리가 이루어지는가?
	최적화	네트워크 전반에서 발생하는 위협에 대하여 즉각적이고 자동화된 대응이 가능한가?
		애플리케이션 프로파일의 변화 등을 탐지하여 동적 네트워크 트래픽 관리가 가능한가?

세부 설명

■ **기존**

✓ **IDS·IPS 등의 솔루션을 도입하여 주요 위협에 대한 감시 체계가 이루어지고 있는가?**

- 침입 탐지/방지 시스템(IDS/IPS) 솔루션을 도입하여 패턴 기반의 시그니처 탐지를 수행하는 단계이다. 실무 환경에서는 외부 또는 내부 네트워크 경계에 IDS/IPS를 설치하여 알려진 공격 패턴(시그니처)과 일치하는 트래픽을 탐지하고 차단하는 기본적인 감시 체계를 운영한다.

✓ **네트워크 정적 규칙에 의한 수동적 트래픽 관리가 이루어지는가?**

- 수동으로 설정된 룰 기반의 ACL 또는 방화벽 정책을 통해 트래픽을 제어한다. 실무 환경에서는 IP 주소, 포트 번호 등을 기준으로 정적인 접근통제 규칙을 설정하며, 이상 트래픽이 발견되면 주로 관리자가 로그를 확인하고 수동으로 차단 정책을 추가하는 등의 조치를 수행한다.

■ **초기**

✓ **자동화된 위협 탐지 및 대응 시스템이 도입되어 보안 이벤트 발생 시 즉각 대응이 가능한가?**

- 기존 IDS/IPS 외에도 SIEM 등의 추가 시스템을 도입, 각 솔루션을 연동하여 보안 이벤트가 발생하면 즉각적으로 관리자에게 알림을 보내는 등의 조치를 수행한다.

✓ **애플리케이션 프로파일에 따른 트래픽 관리가 이루어지는가?**

- 트래픽 흐름을 단순 IP 주소(L3)나 포트(L4) 기반이 아닌 애플리케이션 기반(L7)으로 분류하고, 각

애플리케이션 단위의 정상적인 트래픽 흐름을 모니터링 기반으로 프로파일링하여 정책을 적용하기 시작한다. 실무 환경에서는 NGFW 등을 활용하여 특정 애플리케이션(예시: 그룹웨어, ERP 등)을 식별하고, 해당 애플리케이션의 정상적인 통신 패턴(허용된 프로토콜, 포트, 통신 대상 등)을 기반으로 트래픽 관리 정책을 수립하여 적용한다.

■ **향상**

✓ **실시간 위협 탐지 및 위협 행위에 대한 선제적 대응 체계가 마련되어 있는가?**

- 머신러닝(ML) 기반의 네트워크 트래픽 패턴 학습과 외부 위협 인텔리전스(CTI) 연동을 통해 실시간으로 위협을 탐지한다. 실무 환경에서는 NDR 시스템 등을 활용하여 패킷 수준에서 위협 행위를 심층 분석하고, SIEM을 확장하여 SOAR의 플레이북 기반으로 특정 IP 차단, 감염된 세그먼트 격리 등 식별된 위협에 대한 자동화된 대응을 수행한다. 이를 통해 선제적인 방어 체계를 구축하기 시작한다.

✓ **네트워크 동적 규칙에 의한 네트워크 트래픽 관리가 이루어지는가?**

- SIEM/SOAR, NDR 등 위협 탐지 시스템을 네트워크 기반의 정책 엔진(SDN 컨트롤러, NGFW/ZTNA, ICAM, 마이크로 세그멘테이션 시스템 등)과 연동한다. 위협이 식별되면 정책 엔진이 방화벽 규칙, SDN 플로우 테이블, ZTNA 접근 정책 등을 동적으로 조정하여 해당 위협 트래픽을 차단하거나 격리하는 등 자동화된 트래픽 관리를 수행한다.

■ **최적화**

✓ **네트워크 전반에서 발생하는 위협에 대하여 즉각적이고 자동화된 대응이 가능한가?**

- 통합 위협 대응 플랫폼(정보보안포털, ICAM, XDR 등)을 구축하여 단일 플랫폼에서 모든 네트워크 트래픽을 관리/모니터링하며, 플랫폼은 각 보안 시스템(EDR, NDR, SIEM/SOAR 등)과 연동되어 발생한 위협에 대해 자동화된 대응을 수행한다. 실무 환경에서는 ML/AI 엔진이 상관 분석을 통해 복합적인 위협을 실시간으로 탐지하고, SOAR 플레이북 등을 통해 관리자 개입 없이 즉각적으로 격리, 차단 등의 조치를 수행한다.

✓ **애플리케이션 프로파일의 변화 등을 탐지하여 동적 네트워크 트래픽 관리가 가능한가?**

- ML/AI을 활용하여 애플리케이션의 정상적인 트래픽 흐름(프로파일)을 학습하고, 애플리케이션 프로파일의 변화나 비정상 흐름을 탐지하면 ICAM, SDN, 마이크로 세그멘테이션 시스템 등과 연동하여 트래픽 경로를 자동으로 변경하거나 해당 애플리케이션 및 워크로드를 격리하는 등의 동적 제어를 수행한다. 이를 통해 애플리케이션 수준의 이상 행위에도 자동화된 대응이 가능해진다.

3.3 트래픽 암호화

항목	3.3.1 트래픽 암호화	
설명	암호화는 네트워크 내에서 데이터의 기밀성을 유지하고, 전송 중인 데이터를 보호하기 위한 기술이다. 이는 SSL/TLS, VPN, 데이터 암호화 및 전송 계층 보안 등을 포함한다.	
성숙단계	기존	내·외부 트래픽 일부 암호화가 가능한가?
		SSL, TLS 등 표준 프로토콜 사용과 VPN 등을 사용하고 있는가?
	초기	네트워크 전반에 걸쳐 암호화 기능이 적용되어 있는가?
		데이터 전송 시 암호화를 필수로 하고 있는가?
	향상	전송 중 데이터 암호화 및 저장된 데이터도 모두 암호화하고 있는가?
		최신 암호화 기술을 적용하고, 고급 암호화 키 관리 시스템이 도입되어 있는가?
	최적화	최신 암호화 기술을 도입하고 성능 저하 없이 데이터 보호가 가능한가?
		통합된 키 관리 시스템을 통하여 안전한 키 관리가 이루어지고 있는가?

세부 설명

■ **기존**

✓ **내·외부 트래픽 일부 암호화가 가능한가?**

- 일부 트래픽에 대해 SSL/TLS 기반의 암호화가 적용되어 있으며, 외부 웹사이트 접속 등 웹 통신은 HTTPS 프로토콜을 사용한다. 그러나 전체 내부 네트워크 통신이나 모든 데이터 경로에 대한 포괄적인 암호화는 이루어지지 않고 있는 상태이다.

✓ **SSL, TLS 등 표준 프로토콜 사용과 VPN 등을 사용하고 있는가?**

- SSL/TLS, SSH, VPN(IPsec, SSL-VPN 등) 등과 같이 일반적인 표준 암호화 프로토콜을 사용하여 특정 네트워크 구간(예시: 망별 방화벽 통신 간 VPN 터널링 활용, 외부 환경에서 접근 시 SSL-VPN 활용한 접근 등)이나 서비스에 대한 암호화를 수행한다.

■ **초기**

✓ **네트워크 전반에 걸쳐 암호화 기능이 적용되어 있는가?**

- 조직 전체 네트워크 및 데이터 흐름에 암호화 정책을 확대 적용하여 평문 통신을 사용하지 않는다. 실무 환경에서는 모든 주요 애플리케이션, 서버 간 통신 및 사용자 연결에 암호화 적용을 구현한다. 예를 들어, 서버 접근 시에는 서버 접근제어 키, SSH 등 암호화 프로토콜이 적용되고, 웹 애플리케이션 접근 시에는 암호화 키를 검증하여 접근한다.

✓ **데이터 전송 시 암호화를 필수로 하고 있는가?**

- 데이터 전송 시 암호화를 기본 정책으로 설정하며, 관리 콘솔, API, 애플리케이션 간 통신에 일관되게 적용한다. 실무 환경에서는 데이터 전송 시 암호화된 VPN 또는 SSL-VPN 터널링 등을 활용하며, FTP, HTTP 등 평문 통신 프로토콜은 사용하지 않는다.

■ **향상**

✓ **전송 중 데이터 암호화 및 저장된 데이터도 모두 암호화하고 있는가?**

- 전송 중 데이터뿐만 아니라 저장 되어 있는 데이터도 암호화를 수행한다. 스토리지, 백업, 로그, DB 등 전사 모든 데이터에 대한 암호화가 이루어진다. 실무 환경에서는 eDRM, AIP, DB암호화 등과 같은 시스템을 통해 데이터 자체를 암호화하고, 해당 시스템을 ZTNA, ICAM 시스템 등과 연동하여 데이터 전송 시 암호화 여부를 이중으로 검증하고 통제할 수 있다. 네트워크 암호화와 데이터 암호화가 이중으로 적용되어 안전한 통신과 데이터 보호를 보장한다.

✓ **최신 암호화 기술을 적용하고, 고급 암호화 키 관리 시스템이 도입되어 있는가?**

- 최신 표준 암호화 기술(예시: TLS 1.3, ECDHE, RSA-4096, RSA-8192 등)이 적용된다. 또한, 키 생성, 배포, 수명 주기 관리, 회전, 폐기 등 암호화 키 라이프 사이클을 중앙에서 관리할 수 있는 키 관리 시스템(KMS) 등이 도입되어 전사적인 키 관리를 운영한다.

■ **최적화**

✓ **최신 암호화 기술을 도입하고 성능 저하 없이 데이터 보호가 가능한가?**

- 성능과 보안을 동시에 충족하는 경량화된 암호화를 구현한다. 하드웨어 가속 등을 통해 암호화 성능을 향상시키며, 암호화 정책이 애플리케이션 성능에 미치는 영향을 최소화한다. PQC(양자내성암호) 알고리즘을 적용하여 양자 컴퓨팅 위협에 대비한 장기 데이터 보호를 수행한다. 실무 환경에서는 QKMS(양자 키 관리 장비), QKD(양자 키 분배 장비), QENC(양자 통신 암호화 장비) 등을 도입하고 PQC 알고리즘을 적용하여, PQC 기반의 터널링, 키 관리, 키 분배 등을 전사적으로 적용한다.

✓ **통합된 키 관리 시스템을 통하여 안전한 키 관리가 이루어지고 있는가?**

- KMS를 확장하여 통합 키 관리 시스템을 통해 정책 기반의 키 관리를 수행하며, PAM, ICAM, ZTNA 등 시스템과 연동하여 네트워크, 시스템, 애플리케이션 접근 시 전사적으로 일관된 키 관리 체계를 적용한다. 또한, SIEM/SOAR 시스템 등과 연동하여 키 생성, 사용, 폐기 등 키 라이프사이클 전반에 대한 모니터링 및 감사 추적성을 강화한다.

3.4 트래픽 관리

항목	3.4.1 데이터 흐름 매핑	
설명	네트워크 내에서 데이터가 어떻게 이동하는지를 시각화하고 분석하는 과정이다. 이를 통해 데이터의 출처, 목적지, 경로 등을 파악하여 보안 정책을 설계하고 위협을 예측할 수 있다.	
성숙단계	기존	데이터 트래픽에 대한 수동적 모니터링을 수행하는가?
		네트워크 내 주요 데이터 흐름을 수동으로 매핑하는가?
	초기	애플리케이션 단위의 트래픽 매핑이 가능한가?
		자동화된 데이터 흐름 매핑 도구를 도입하여 네트워크 내 모든 데이터 흐름이 실시간으로 매핑되는가?
	향상	주요 데이터 트래픽과 관련된 보안 정책이 수립되어 비정상적 데이터 이동을 탐지하는가?
		데이터 흐름에 대한 분석을 상관관계를 통하여 분석하고, 위협을 사전에 식별 가능한가?
	최적화	AI 기반 예측 분석 도구를 활용하여 데이터 흐름의 변화를 실시간으로 감지하는가?
		네트워크 트래픽 우선순위를 동적으로 변경하고 구성할 수 있는가?

세부 설명

■ **기존**

✓ **데이터 트래픽에 대한 수동적 모니터링을 수행하는가?**

- 트래픽 흐름에 대한 시스템 자체적인 로그 수집, 방화벽 룰, 스위치 포트 미러링 등의 방식을 사용하여 수동으로 데이터 흐름을 모니터링한다. 실무 환경에서는 방화벽이나 IPS, 또는 시스템(서버) 자체에서 네트워크 트래픽 기반의 기본적인 데이터 흐름을 모니터링하고, 이상 징후 발견 시 수동적인 조치(예시: 방화벽 정책 변경)를 수행하는 단계이다.

✓ **네트워크 내 주요 데이터 흐름을 수동으로 매핑하는가?**

- 주요 서버, DB, 클라이언트 간 데이터 흐름을 주로 관리자의 경험에 의존하여 수동으로 매핑한다. 실무 환경에서는 네트워크 구성도나 데이터 흐름도 등을 수기로 작성하여 관리하고 업데이트하며, 실제 트래픽 흐름과의 일치 여부를 실시간으로 검증하기 어렵다. 통신 경로에 대한 보안 정책 적용은 미흡한 상태이다.

■ **초기**

✓ **애플리케이션 단위의 트래픽 매핑이 가능한가?**

- NMS 등을 통해 기본적인 네트워크 트래픽을 모니터링하고, 트래픽 흐름을 사용자 및 애플리케이션 단위로 분류하여 매핑하기 시작한다. 실무 환경에서는 주요 자산 간 흐름 파악을 넘어, 특정 애플리케이션(예시: ERP, 그룹웨어 등)과 관련된 데이터 흐름을 식별하는 수준을 의미한다. 매핑된 결과는 마이크로 세그멘테이션 정책 수립 등의 기초 자료로 활용될 수 있다.

✓ **자동화된 데이터 흐름 매핑 도구를 도입하여 네트워크 내 모든 데이터 흐름이 실시간으로 매핑되는가?**

- 네트워크 트래픽 분석 도구 또는 NMS 등의 시스템을 활용하여 자동으로 데이터 흐름을 매핑하고 실시간으로 업데이트하여 관리한다. 실무 환경에서는 수동으로 다이어그램을 그리는 대신, 시스템이 자동으로 생성·갱신하는 데이터 흐름도나 네트워크 다이어그램 등을 활용하여 현재의 통신 경로와 데이터 이동 현황을 파악할 수 있다.

■ **향상**

✓ **주요 데이터 트래픽과 관련된 보안 정책이 수립되어 비정상적 데이터 이동을 탐지하는가?**

- 노드 간의 관계나 접속 패턴을 기반으로 주요 데이터 트래픽에 대한 보안 정책을 수립하며, eDLP, AIP, ICAM, ZTNA 등의 시스템과 연동하여 정형화된 데이터 흐름에 대한 정상 기준(Baseline)을 바탕으로 비정상적인 데이터 이동을 탐지한다. 실무 환경에서는 NDR을 통해 풀 패킷 기반으로 네트워크 흐름을 분석하여 정상 기준을 설정하고, 이 기준을 벗어나는 비정상적인 데이터 이동(예시: 대량의 내부 자료 외부 전송 시도 등)을 탐지 시 SIEM/SOAR와 연계하여 관리자에게 알람을 보내거나 관련 조치를 수행할 수 있다.

✓ **데이터 흐름에 대한 분석을 상관관계를 통하여 분석하고, 위협을 사전에 식별 가능한가?**

- 네트워크 트래픽 흐름, 사용자 ID, 위치, 시간, 접속 포트 등을 연계한 상관 분석을 수행하여 비정상적인 데이터 흐름을 조기에 탐지한다. 실무 환경에서는 NDR, XDR 시스템 등을 활용해 풀 패킷 기반으로 네트워크 흐름 및 상관관계 분석을 수행하고, SIEM/SOAR 연계를 통해 비정상적인 데이터 이동 탐지 시 관리자 알람 또는 자동화된 조치를 수행한다. 또한, 외부 위협 인텔리전스(CTI) 정보와 연동하여 알려진 악성 IP/URL과의 통신 시도 등 외부 위협과 관련된 데이터 흐름을 식별하고 사전에 차단할 수 있다. 탐지된 위협 정보는 정책 엔진에 반영되어 실시간으로 업데이트될 수 있다.

■ **최적화**

✓ **AI 기반 예측 분석 도구를 활용하여 데이터 흐름의 변화를 실시간으로 감지하는가?**

- ML/AI를 기반으로 정상/비정상 데이터 흐름 패턴을 학습하여 새로운 이상 징후를 실시간으로 탐지한다. 실무 환경에서는 NDR, XDR 등의 시스템이 ML/AI 엔진을 활용하여 데이터 흐름의 지속적으로 모니터링하여 데이터 흐름 변화를 실시간으로 감지하고 알려지지 않은 위협 패턴까지 예측 분석하여 즉각적이고 자동화된 대응이 가능하다.

✓ **네트워크 트래픽 우선순위를 동적으로 변경하고 구성할 수 있는가?**

- 데이터 흐름 분석 결과를 ICAM, ZTNA, 마이크로 세그멘테이션, XDR, SIEM/SOAR 등 다양한 시스템과 유기적으로 연동하여 자동화된 대응 체계를 구축한다. 실무 환경에서는 AI가 식별한 위협이나 비정상 흐름에 따라 SOAR 플레이북 등을 통해 특정 트래픽을 자동으로 격리하거나, 비즈니스 중요도에 따라 ICAM, ZTNA, 마이크로 세그멘테이션 시스템 등을 통해 트래픽 우선순위를 실시간으로 조정하는 등 데이터 흐름에 따라 트래픽 관리가 동적으로 이루어진다.

3.5 네트워크 회복성

항목	3.5.1 네트워크 회복성	
설명	네트워크 회복성은 네트워크가 다양한 위협이나 장애로부터 신속하게 복구하고, 지속적으로 가용성을 유지할 수 있도록 하는 능력이다. 이 기능은 다중 경로 설계, 자동 복구, 재해 복구 계획 등을 포함한다.	
성숙단계	기존	애플리케이션 및 워크로드에 대한 기본적인 복구 계획과 백업 경로가 마련되어 있는가?
		재해 복구에 대한 주기적 백업 실시가 이루어지는가?
		네트워크 장비에 대한 장애 대응 절차가 수립되어 있는가?
	초기	네트워크 내 다중 경로가 설계되어 있고, 자동 복구 시스템이 도입되어 있는가?
		자동화된 장애 조치(Failover) 메커니즘이 적용되어 있는가?
		네트워크 이중화 설계가 되어 있는가?
	향상	네트워크가 장애나 공격에도 지속적으로 서비스 지원이 가능한가?
		재해 복구 계획에 따라 주기적으로 테스트하여 항상 준비 상태가 유지되어 있는가?
	최적화	어떠한 상태에서도 네트워크 서비스의 중단 없이 지속적 운영이 가능한가?
		네트워크 장애를 실시간으로 감지하고 복구하며, 모든 복구 절차를 자동화하였는가?

세부 설명

■ **기존**

✓ **애플리케이션 및 워크로드에 대한 기본적인 복구 계획과 백업 경로가 마련되어 있는가?**

- 장애 발생 시 수동 복구를 수행할 수 있도록 주요 시스템 및 애플리케이션을 식별하고 이에 대한 기본적인 복구 절차와 백업 경로가 문서 형태로 마련되어 있다. 실무 환경에서는 BCP(업무 연속성 계획) 및 DRP(재해 복구 계획) 개념이 정보보안 정책 등에 반영되어 있으나, 실제 복구 과정은 자동화되지 않고 수동 절차에 의존한다.

✓ **재해 복구에 대한 주기적 백업 실시가 이루어지는가?**

- 복구를 목적으로 수동 백업을 주기적(예시: 일/주 단위)으로 진행한다. 중요 데이터의 경우 정책을 수립하여 이중 백업, 소산 백업이나 외부 저장소(DR 센터 등) 저장을 적용할 수 있다. 백업 및 복구 과정은 주로 수동으로 관리된다.

✓ **네트워크 장비에 대한 장애 대응 절차가 수립되어 있는가?**

- 중요 네트워크 장비(예시: 라우터, 방화벽 등 게이트웨이 역할 장비)를 식별하고 이에 대한 장애 대응 절차가 수립되어 있다. 실무 환경에서는 일부 중요 장비에 한해 기본적인 이중화가 구성되어 있거나, 유휴 장비를 활용한 수동 전환 또는 교체 절차가 문서화 되어 있는 수준이다.

■ **초기**

✓ **네트워크 내 다중 경로가 설계되어 있고, 자동 복구 시스템이 도입되어 있는가?**

- 라우팅 프로토콜(RIP/OSPF/BGP 등)을 통해 링크 장애를 대비한 대체 경로를 확보하며, LACP 등으로 물리적인 링크를 이중화(본딩)하거나 STP 등으로 물리적으로 이중화된 경로 환경에서 루프를 방지하고 대체 경로를 확보하여 네트워크 인프라를 구성한다. 네트워크 경로 또는 시스템 장애가 발생하면 프로토콜에 의해 자동으로 대체 경로가 활성화되어 기본적인 복구가 이루어진다.

✓ **자동화된 장애 조치(Failover) 메커니즘이 적용되어 있는가?**

- Failover 메커니즘을 바탕으로 네트워크 장비 또는 시스템 장애가 발생하면 자동으로 예비 시스템(Standby)이 작동(Active)하여 서비스 중단 시간을 최소화하는 구성이 적용되기 시작한다. 실무 환경에서는 인라인(Inline) 보안 장비 등의 장애 시 트래픽 흐름을 유지하기 위한 S/W 바이패스나 H/W 바이패스 기능, 또는 라우터/방화벽 등에서 Active-Standby 이중화 구성을 통해 주 장비(Active) 장애 시 예비 장비(Standby)로 트래픽을 자동으로 넘기는 메커니즘 등이 이에 해당한다.

✓ **네트워크 이중화 설계가 되어 있는가?**

- 네트워크 구성상 이중 스위치 및 다중 라우터 등을 구성하여 단일 또는 일부 네트워크 장비 장애 시 서비스 영향 범위를 최소화하는 이중화 설계가 적용된다. 실무 환경에서는 내부 네트워크의 설계와 구성을 고려하여 이중화 설계가 반영되어 있으며, 장애 발생 시 장애 대응 절차에 따라 조치가 이루어진다. 또한, 기본적인 위협 발생 시 라우팅 경로 등을 수정하여 조치할 수 있는 체계가 마련되기 시작한다.

■ **향상**

✓ **네트워크가 장애나 공격에도 지속적으로 서비스 지원이 가능한가?**

- 네트워크 장애 및 공격 발생 후에도 비즈니스와 연관된 주요 서비스가 중단되지 않도록 논리적 및 물리적 회복성을 모두 고려하여 네트워크 구성을 Active-Active 또는 Active-Standby 이중화 구조로 구성하고, 장애 발생 시 자동화된 복구 절차가 즉각적으로 수행된다. 실무 환경에서는 RPA 등을 활용하여 백업 관리 시스템과 연동된 자동 복구 스크립트를 실행하거나, SDN 환경에서 동적으로 트래픽 경로를 재설정하는 등의 조치를 통해 서비스 연속성을 보장한다.

✓ **재해 복구 계획에 따라 주기적으로 테스트하여 항상 준비 상태가 유지되어 있는가?**

- 주기적으로(예:시 반기별, 연간) DR(재해 복구) 시나리오 기반의 모의 테스트를 수행하여 복구 절차의 유효성을 검증한다. 실무 환경에서는 핫 사이트 또는 웜 사이트 수준의 DR 환경을 구축하고, 실제 재해 상황을 가정한 테스트를 통해 복구 절차의 문제점을 식별하고 개선한다. 테스트 결과를 기반으로 복구 목표 시간(RTO) 및 복구 목표 시점(RPO)을 최적화하고 항상 준비 상태를 유지한다.

■ **최적화**

✓ **어떠한 상태에서도 네트워크 서비스의 중단 없이 지속적 운영이 가능한가?**

- 네트워크의 모든 구성 요소가 이중화되어 있으며, 장애 및 공격 발생 시 자동으로 정상 네트워크 경로로 전환하고 복구 절차를 수행한다. 또한 전체 서비스 가용성을 실시간으로 모니터링하고, ML/AI 기반 분석 결과에 따라 ICAM, ZTNA, 마이크로 세그멘테이션, XDR, SIEM, SOAR 등의 다양한

시스템과 자동으로 연동되어 트래픽을 선제적으로 분산하고, 부하로 인한 장애를 사전에 차단하는 등 어떠한 상황에도 탄력적인 운영이 가능한 자율적인 시스템 환경을 구축한다.

✓ **네트워크 장애를 실시간으로 감지하고 복구하며, 모든 복구 절차를 자동화하였는가?**

- ML/AI를 바탕으로 실시간으로 네트워크 장애를 예측하고 탐지하며, 장애 탐지 시 자동으로 네트워크 경로를 전환하고 모든 복구 절차를 관리자 개입 없이 수행한다. NDR, ICAM, ZTNA, 마이크로 세그멘테이션, XDR, SIEM, SOAR과 네트워크 구성이 연동되어 장애 발생 예측 시점부터 복구 완료까지 전 과정이 자동화되어 운영된다.

4. 시스템

4.1 접근통제

항목	4.1.1 접근통제	
설명	사용자와 기기가 네트워크와 시스템에 접근할 때, 허용된 자원만을 사용할 수 있도록 권한을 부여하고 이를 엄격하게 관리하는 보안 기능이다. 이를 통해 적절한 자격을 가진 사용자만이 필요한 리소스에 접근할 수 있으며, 보안 사고를 예방할 수 있다.	
성숙단계	기존	사용자 및 기기에 수동으로 권한을 부여하는가?
		RBAC 기반 접근제어를 수행하는가?
		권한 관리를 수동으로 수행하는가?
	초기	역할과 권한 기반으로 중앙 집중형으로 권한 부여가 가능한가?
		실시간 접근권한 부여가 가능한가?
		권한 변경 사항이 자동으로 반영되는가?
		특정 리소스에 대한 접근 제한·승인 정책이 자동으로 적용 가능한가?
	향상	ABAC 기반 접근제어를 수행하는가?
		다양한 조건을 바탕으로 세밀하고 동적으로 실시간 접근권한이 부여되는가? (위치, 기기 상태, 시간 등)
	최적화	사용자·기기의 상태를 실시간으로 분석하고 실시간·자동으로 권한 조정이 가능한가?
		모든 접근제어는 중앙집중적인 시스템에서 실시간으로 관리되는가?
		시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정이 가능한가?
		위험 분석 기반 지속적인 접근제어 정책이 도입되어 있는가?

세부 설명

■ **기존**

✓ **사용자 및 기기에 수동으로 권한을 부여하는가?**

- 관리자가 사용자/기기별로 수동으로 시스템에 대한 접근권한을 설정한다. 실무 환경에서는 개별 시스템(예시: 윈도우, 리눅스 서버)에서 로컬 계정을 직접 생성하거나, 접근권한 대장을 스프레드시트 등으로 관리자가 수동 관리함을 의미한다. 이 방식은 권한 부여/회수가 실시간으로 반영되지 않으며, 인적 실수로 인한 리스크가 존재한다.

✓ **RBAC 기반 접근제어를 수행하는가?**

- 미리 정의된 사용자 역할(Role)에 따라 접근권한을 부여하며, 역할별 접근권한에 따른 제어를 수행한다. 실무 환경에서는 Directory의 보안 그룹이나 개별 시스템의 사용자 그룹을 활용하여 '개발자', '운영자' 등 미리 정의된 역할(Role)에 따라 접근권한을 부여한다.

✓ **권한 관리를 수동으로 수행하는가?**

- 권한의 생성, 부여, 변경, 폐기 등의 관리를 수동으로 수행하여 이력 추적이나 실시간 반영이 어려운 상태이다. 실무 환경에서는 권한 요청을 이메일이나 그룹웨어 결재, IT 헬프데스크 티켓 등으로 처리하더라도, 최종적인 작업은 관리자가 각 시스템에 접속하여 수동으로 수행함을 의미한다.

■ **초기**

✓ **역할과 권한 기반으로 중앙 집중형으로 권한 부여가 가능한가?**

- 권한 관리를 위한 중앙 집중형 시스템(시스템 접근제어, DB 접근제어, IAM 등)을 구축하고, 이 시스템이 Directory, HRM 등 계정 관련 솔루션과 연동되어 사용자 역할(Role)에 따른 권한을 중앙 시스템에서 일괄적으로 부여하고 관리하기 시작한다.

✓ **실시간 접근권한 부여가 가능한가?**

- 사용자가 그룹웨어나 IAM 등 시스템의 포털 등을 통해 권한을 요청할 경우, 승인 절차를 거쳐 사용자 정보를 기반으로 관리자가 승인 여부를 판단하고 권한을 부여할 수 있으며, 이를 통해 수동 작업 대비 리소스 접근에 소요되는 시간을 단축한다.

✓ **권한 변경 사항이 자동으로 반영되는가?**

- 사용자 정보 변경(부서 이동, 직무 변경, 퇴사 등)이 HRM(인사관리) 시스템 등에 반영되면 해당 정보를 연동된 중앙 집중형 시스템(Directory, IAM 등)에서 RBAC 정책에 따라 권한을 자동으로 반영하거나 PAM(시스템 접근제어, DB 접근제어 등) 시스템의 권한을 회수하는 등 신규 역할에 맞는 권한을 재부여하여 권한 변경 사항을 반영할 수 있다.

✓ **특정 리소스에 대한 접근 제한·승인 정책이 자동으로 적용 가능한가?**

- PAM(시스템 접근제어, DB 접근제어) 시스템 등에서 조직 내 주요 리소스(예시: 운영 서버, 고객 DB 등) 접근 시, IAM 등 중앙 시스템의 사용자 역할 정보를 기반으로 사전에 정의된 정책을 자동으로 적용한다. 실무 환경에서는 'user' 권한은 역할 기반(예시: '운영팀' 그룹)으로 자동 승인하되, 'root' 또는 'DBA' 권한은 별도 승인 절차(예시: 그룹웨어 결재 연동)를 거치도록 접근을 제한하는 정책을 의미한다.

■ **향상**

✓ **ABAC 기반 접근제어를 수행하는가?**

- RBAC(역할 기반 접근제어)에서 확장되어, 사용자 역할(Role) 외에도 다양한 속성(Attribute) 정보를 기반으로 권한 정책을 설정하는 ABAC(속성 기반 접근제어)를 도입하여 접근제어를 수행한다. 여기서 다양한 속성이란 사용자 속성(예시: 부서, 직책, 보안 등급), 리소스 속성(예시: 데이터 민감도, 파일 형식), 환경 속성(예시: 접속 시간, 위치, 기기 보안 상태) 등을 의미한다. 실무 환경에서는 이러한 속성들을 조합하여 'IF [사용자 속성 AND 리소스 속성 AND 환경 속성] THEN [허용/거부]' 와 같은 형식의 정교한 접근 규칙을 정책 엔진(예시: ICAM, PAM)에 설정한다. 예를 들어, 동일한 '인사팀' 역할이라도 '근무 시간 중'이고 '사내망'에서 접속하며 '보안 업데이트 완료된 기기'를 사용할 때만 '급여 정보 수정' 권한을 부여하는 식으로, 단순 역할뿐만 아니라 다양한 속성을 실시간으로 평가하여 접근제어를 수행한다.

✓ **다양한 조건을 바탕으로 세밀하고 동적으로 실시간 접근권한이 부여되는가?(위치, 기기 상태, 시간 등)**

- 사용자의 위치, 접속 기기의 보안 상태(예시: 필수 S/W 설치 여부, 사용자 별 스코어링), 접속 시간대 등 상황별 속성(컨텍스트) 정보를 바탕으로 세분화된 접근 정책을 정의한다. 실무 환경에서는 ICAM, ZTNA, PAM 등 중앙 시스템의 정책 엔진이 이러한 속성 정보를 실시간으로 모니터링하여 접근권한을 동적으로 조정한다. 예를 들어, 동일한 '운영자' 역할이라도 '사무실' 위치에서는 모든 시스템 접근을 허용하지만, '외부'에서 '미등록 기기'로 접속 시에는 접근을 차단하는 등 세밀한 제어를 수행한다.

■ **최적화**

✓ **사용자·기기의 상태를 실시간으로 분석하고 실시간·자동으로 권한 조정이 가능한가?**

- ML/AI 기반 분석을 바탕으로 사용자 행동 및 기기 상태를 실시간으로 분석하고 이상 징후 탐지 시 자동으로 권한을 회수하거나 접근을 제한하는 등의 조치를 수행한다. 실무 환경에서는 SIEM/SOAR의 UEBA 기능 등을 활용해 시스템이 지속적으로 사용자 및 기기의 위험 점수를 스코어링하고, 이 점수가 임계치를 넘어서면 ICAM, PAM, ZTNA 등 정책 엔진과 연동하여 관리자 개입 없이 권한을 즉시 조정한다.

✓ **모든 접근제어는 중앙집중적인 시스템에서 실시간으로 관리되는가?**

- 접근 요청의 승인, 정책 적용 등 접근제어를 위한 모든 기반 정보가 중앙 시스템(ICAM, 정보보안 포털 등)에서 실시간으로 수집되고, 전사 내 모든 시스템(온프레미스, 클라우드, SaaS 포함)에 대한 접근제어를 PAM 등을 통하여 일괄 관리하여 접근제어를 관리한다.

✓ **시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정이 가능한가?**

- 시스템에 영향을 미치는 특정 명령어(예시: rm -rf, shutdown) 실행 시 사용자의 신뢰 점수를 실시간으로 재평가한다. 실무 환경에서는 PAM 시스템 등이 명령어 실행 요청을 가로채 정책 엔진(ICAM, SIEM/SOAR 등)에 신뢰도 재평가를 요청하고, 신뢰도 기준 미달 시 강화된 추가 인증(MFA)을 요구하거나 해당 명령어 실행을 제한하는 등의 조치를 수행한다.

✓ **위험 분석 기반 지속적인 접근제어 정책이 도입되어 있는가?**

- 외부 위협 인텔리전스(CTI) 등 새로운 위험 정보는 즉각적으로 학습하여 정책 엔진(ICAM, SIEM/SOAR 등)에 반영하며, 시스템 접근 대상자에 대한 실시간 위험 평가를 수행하여 그 결과를 바탕으로 PAM 시스템 등을 통해 지속적인 접근제어를 수행한다. 실무 환경에서는 ML/AI를 활용해 위험 예측 분석을 수행하고, 분석 결과를 바탕으로 접근 정책이 자율적으로 조정되는 수준을 의미한다.

4.2 시스템 계정 관리

항목	4.2.1 PAM	
설명	PAM은 권한 있는 사용자 및 시스템의 접근을 관리하고 모니터링하는 보안 체계로, 영구적인 관리자/높은 권한을 제거하는데 중점을 두며, 이를 위해 먼저 특권 계정 관리(PAM) 시스템을 구축하고, 권한 사용자를 이 시스템으로 이전하는 작업을 수행한다. 이후, 권한 상승 승인을 자동화하고, 시스템에 분석 데이터를 입력하여 이상 탐지를 수행하는 방식으로 사용된다.	
성숙단계	기존	PAM 시스템을 구축하였는가?
		PAM 정책이 수립되어 있는가?
	초기	PAM 솔루션을 통해 사용자 접근을 모니터링하고 제어 가능한가?
		자동화된 권한 상승 승인 기술이 도입되어 있는가?
	향상	PAM 솔루션을 통해 비정상적 활동이 탐지 가능한가?
	최적화	AI 기반 위협 탐지 및 대응 기능을 활용하여 PAM 시스템에 적용하였는가?

세부 설명

■ **기존**

✓ **PAM 시스템을 구축하였는가?**

- 관리자 계정, 시스템 계정 등 권한이 있는 사용자 계정을 별도로 식별하고, 시스템 접근제어 또는 DB 접근제어 시스템과 같은 기본적인 PAM 시스템을 도입하여 계정 관리를 시작하는 단계이다. 실무 환경에서는 이러한 시스템을 통해 특권 계정의 생성, 부여, 폐기 등을 관리하지만, 전사적인 통합 관리보다는 개별 시스템 단위 또는 특정 영역(예시: 서버 관리)에 한정되어 적용되는 경우가 많다.

✓ **PAM 정책이 수립되어 있는가?**

- 권한 계정 사용 조건(사용자, 대상 시스템, 시간대 등), 승인 절차, 권한 유효 기간 등의 기본적인 접근 정책을 문서화하고, 도입된 PAM 시스템상에 정적인 규칙으로 반영한다. 이 단계에서는 정책이 주로 수동으로 관리되며, 실시간 상황 변화에 따른 동적인 정책 조정은 이루어지지 않는다.

■ **초기**

✓ **PAM 솔루션을 통해 사용자 접근을 모니터링하고 제어 가능한가?**

- 권한 계정으로의 로그인, 명령어 실행, 세션 기록 등을 실시간으로 모니터링하고, 사전에 정의된 정책 위반(예시: 금지 명령어 실행 시도) 모니터링하여 PAM 시스템을 통해 해당 세션을 강제 종료하거나 특정 명령어 실행을 차단하는 등 초기 수준의 중앙 제어가 가능하다. 실무 환경에서는 시스템 접근제어 또는 DB 접근제어 솔루션의 감사 로그 및 세션 모니터링 기능을 활용한다.

✓ **자동화된 권한 상승 승인 기술이 도입되어 있는가?**

- PAM 시스템을 IAM, 그룹웨어 결재 시스템 등 계정 및 접근권한 관리 시스템과 연동하여, 사용자

정보를 기반으로 권한 요청에 대한 승인 여부를 PAM 시스템상에서 판단하고 기본적인 자동화를 통해 권한을 부여할 수 있다. 실무 환경에서는 사용자가 포털 등을 통해 특정 시간 동안 특정 시스템에 대한 권한 상승을 요청하면, 승인 절차(예시: 그룹웨어 결재 완료 시 IAM에서 계정과 권한 부여) 후 PAM 시스템이 자동으로 상승된 권한을 일시 부여하여 시스템 접근을 제어하는 수준을 의미한다.

■ **향상**

✓ **PAM 솔루션을 통해 비정상적 활동이 탐지 가능한가?**

- PAM 시스템을 IAM, ICAM 시스템과 같은 계정 및 접근권한 시스템 외에도 XDR, SIEM/SOAR 등의 시스템과 연동하여 비정상적인 활동을 탐지한다. 실무 환경에서는 PAM 시스템의 로그(예시: 평소와 다른 시간대의 로그인 시도, 과도한 실패 시도, 비정상적인 명령어 실행 등)를 SIEM/SOAR로 전송하여 다른 시스템의 로그와 상관 분석을 수행한다. 보안 이벤트 발생 시 즉각적으로 관리자에게 알림을 보내거나 SOAR 플레이북이나 PAM 자체적인 기능을 통해 자동화된 조치(예시: 의심 계정 임시 잠금)를 수행할 수 있다. 또한, 권한 요청, 승인, 사용, 폐기의 전 과정에 대한 절차 및 감사 로그 기록을 강화하여 주기적인 분석을 수행하고 위협 탐지를 정교화한다.

■ **최적화**

✓ **AI 기반 위협 탐지 및 대응 기능을 활용하여 PAM 시스템에 적용하였는가?**

- 권한과 계정 및 접근제어의 이상 사용 패턴을 ML/AI을 기반으로 실시간으로 분석하며, 이상 사용 패턴 탐지 시 자동으로 접근 차단, 추가 인증 요구, 세션 강제 종료 등의 조치를 수행한다. 실무 환경에서는 시스템 접근제어, DB 접근제어, 쿠버네티스 환경 접근제어 및 IDP 연계를 통한 애플리케이션(업무 시스템)의 특권 계정 권한 관리와 접근제어가 전사적으로 통합된 PAM 시스템으로 통합되어 이루어진다. 해당 통합 PAM 시스템은 SIEM/SOAR, EDR, ICAM, ZTNA 등과 유기적으로 연동되어, ML/AI가 사용자 및 시스템의 평소 행동 패턴을 학습하고 실시간으로 분석한다. 이상 징후(예시: 휴면 계정의 비정상적 로그인 시도, 과도한 권한 상승 요청, 알려진 악성 행위 패턴과 일치하는 명령어 실행 등) 탐지 시, 관리자 개입 없이 자동으로 접근을 차단하거나 세션을 종료하는 등 자율적인 위협 대응을 수행한다. 또한 보안 위협 동향, 내부 감사 결과, 이상 징후 분석 결과 등을 지속적으로 학습하여 PAM 정책을 자동으로 업데이트하고 최적화한다.

항목	4.2.2 자격 증명 관리	
설명	자격 증명 관리는 사용자와 기기의 인증 정보를 안전하게 저장하고 관리하는 기능으로, 이를 통해 네트워크 및 시스템 접근 시 올바른 자격 증명이 이루어지도록 한다. 이는 패스워드, 인증서, 다중 인증(MFA) 등을 포함한다.	
성숙단계	기존	자격 증명이 수동으로 관리되는가?
		패스워드에 기반한 인증 방식에 의존하는가?
		자격 증명 관리가 체계적이지 않고 수동적인가?
	초기	자격 증명 시스템이 중앙에서 관리되며 자동화되는가?
		MFA 등 보다 안전한 인증 방식이 적용되어 있는가?
	향상	생체 인증 등 고급 인증 방식이 도입되어 있는가?
		자격 증명 관리 시스템을 고도화하여 관리하는가?
		자격 증명의 무결성을 보장하고 인증 프로세스가 강화되었는가?
		AI 기반으로 실시간으로 인증정보 분석이 가능한가?
	최적화	비정상적인 인증 시도를 실시간으로 차단 가능한가?
		실시간으로 인증 정책 조정이 가능한가?
		모든 자격 증명 데이터가 중앙관리되며, 자율적으로 운영되는가?

세부 설명

■ **기존**

✓ **자격 증명이 수동으로 관리되는가?**

- 사용자 계정, 패스워드, 인증서 등 자격 증명 정보가 스프레드시트 등에 수기로 관리된다. 실무 환경에서는 초기 패스워드 발급, 인증서 갱신 등의 작업이 관리자에 의해 수동으로 처리되며, 자동화된 관리 체계가 부재하다.

✓ **패스워드에 기반한 인증 방식에 의존하는가?**

- 시스템 접근 시 단일 ID/패스워드 방식에 주로 의존하며, MFA(다중 인증)와 같은 추가 인증 방식은 개별 시스템이나 일부만 제한되어 적용되어 있다. 패스워드 정책 시 복잡도 요구사항이 낮거나 주기적인 변경이 강제되지 않는 등의 리스크를 보유하고 운영된다.

✓ **자격 증명 관리가 체계적이지 않고 수동적인가?**

- 중앙 시스템을 통한 통합 자격 증명 관리는 구축되지 않았으며, 각 시스템 또는 서비스별로 자격 증명 관리가 개별적이고 분산되어 진행된다. 계정 생성, 권한 회수, 계정 비활성화/삭제 등 자격 증명 라이프사이클 관리에 대한 체계적인 정책이나 자동화된 절차가 정의되지 않은 상태이다.

■ **초기**

✓ **자격 증명 시스템이 중앙에서 관리되며 자동화 되는가?**

- 자격 증명 관리를 위한 중앙 관리 시스템(IAM, ICAM 등)이 도입되어 자격 증명을 통합 관리하기 시작하며, 생성, 배포, 폐기 등 기본적인 관리 프로세스가 시스템을 통해 자동화되기 시작한다. 실무 환경에서는 Directory 계정 생성 시 초기 패스워드가 자동으로 발급되거나, 퇴사 시 계정이 자동으로 비활성화되는 등 초기 수준의 기초적인 자동화가 적용되는 단계를 의미한다.

✓ **MFA 등 보다 안전한 인증 방식이 적용되어 있는가?**

- 기존 패스워드 방식 외에 OTP, 인증 앱 등 추가적인 인증 수단을 도입하여 MFA(다중 인증)를 수행한다. 인증 방식에 대한 정책(예시: 관리자 계정 필수 적용, 원격 접속 시 적용 등)을 정의하고 중앙 관리 시스템(SSO, IAM, ICAM, 시스템/DB 접근제어 등)에 반영하여 전사적으로 일관된 자격 증명 및 인증 정책을 적용하기 시작한다.

■ **향상**

✓ **생체 인증 등 고급 인증 방식이 도입되어 있는가?**

- 지문, 얼굴 인식, 홍채 스캔 등의 생체정보 기반 인증 수단(FIDO2 등)을 도입하여 사용자별 인증 수단을 다양화하고 Passwordless 환경을 구축하기 시작한다. 실무 환경에서는 다양한 시스템에 ICAM 또는 MFA 솔루션과 연동하여, 사용자가 패스워드 없이 생체정보만으로 안전하게 인증할 수 있도록 지원한다.

✓ **자격 증명 관리 시스템을 고도화하여 관리하는가?**

- 중앙화된 자격 증명 관리 시스템(ICAM, MFA 시스템 등)과 정책 엔진(예시: ICAM, ZTNA, PAM 등)을 연동하여 정책에 따라 자격 증명 갱신, 유출 탐지(예시: 다크웹 모니터링 연동), 강제 회수(예시: 퇴사자 발생 시 즉시 비활성화) 등을 즉각적으로 수행하는 등 고도화된 관리 기능을 구현한다. 실무 환경에서는 주기적인 패스워드 변경 강제, 유출된 자격 증명 사용 시도 시 알림 및 자동 잠금 등의 기능이 이에 해당한다.

✓ **자격 증명의 무결성을 보장하고 인증 프로세스가 강화되었는가?**

- 자격 증명 정보(패스워드, 생체정보, 인증서 등)는 암호화되어 안전하게 저장(암호화 적용)되며, 위·변조 탐지 메커니즘을 통해 자격 증명 정보의 무결성을 검증한다. 실무 환경에서는 저장된 패스워드 해시값이나 인증서 파일의 무결성 등을 주기적으로 검증하고, 자격 증명 정보가 업데이트되면 실시간으로 중앙 시스템에 반영되어 인증 프로세스가 강화된다.

✓ **AI 기반으로 실시간으로 인증정보 분석이 가능한가?**

- 인증 패턴, 사용자 위치, 시간대 등 다양한 컨텍스트 정보를 ML/AI을 통해 실시간으로 분석하여 비정상적인 인증 시도(예시: Credential Stuffing, Impossible Travel 등)를 탐지한다. 실무 환경에서는 ICAM 이나 SIEM/SOAR의 UEBA 기능 등을 활용하여 위험도를 스코어링하고, 탐지된 이상 징후는 관리자 알림 또는 자동화된 대응(예시: 계정 잠금)으로 이어질 수 있다.

■ **최적화**

✓ **비정상적인 인증 시도를 실시간으로 차단 가능한가?**

- 사용자 인증 시도 시 ML/AI 기반의 UEBA 기능이 실시간으로 적용되어 비정상 시도(예시: Credential Stuffing, Impossible Travel 등)를 즉시 감지한다. 실무 환경에서는 감지된 비정상 시도에 대해 ICAM, ZTNA 등 정책 엔진과 SIEM/SOAR가 연동되어, 사전에 정의된 정책에 따라 관리자의 개입 없이 자동으로 추가 인증(MFA)을 요구하거나 해당 계정의 접근을 즉시 제한(차단)하는 등의 조치를 실시간으로 수행한다.

✓ **실시간으로 인증 정책 조정이 가능한가?**

- ML/AI를 기반으로 사용자 행동, 접속 환경(기기 상태, 위치, 시간 등)에 따른 위험을 실시간으로 분석하고, 각 상황에 따른 사용자 및 기기의 동적인 위험 점수를 스코어링한다. 이러한 스코어링 결과는 실시간으로 정책 엔진(예시: ICAM, ZTNA, PAM 등)에 반영되어, 단순히 접근 허용/차단을 넘어 인증 강도(예시: 위험도 낮으면 Passwordless, 높으면 MFA)나 인증 방식을 동적으로 조정하는 정책을 수행한다.

✓ **모든 자격 증명 데이터가 중앙관리 되며, 자율적으로 운영되는가?**

- 전사 모든 자격 증명 정보(패스워드, 인증서, API 키, 생체정보 등)가 하나의 중앙 시스템(ICAM 등)을 통해 일괄 관리된다. 계정 생성, 권한 부여, 인증서/키 갱신 및 폐기, 권한 만료 등 자격 증명 라이프사이클 관리 프로세스 전체가 중앙 시스템을 통해 자동으로 수행(예시: 입사자 발생 시 HRM을 연동해 필요 인증서, 키 자동 생성/폐기, 정책 기반 자동 갱신/회전)된다. 이 중앙 시스템은 SIEM/SOAR, PAM, ZTNA 시스템 등과 유기적으로 연동되어, ML/AI가 자격 증명 사용 패턴, 유효 기간, 관련 위협 정보 등을 지속적으로 분석한다. 분석 결과를 바탕으로 정책을 자동으로 업데이트하고, 위험 예측(예시: 곧 만료될 인증서, 휴면 계정의 비정상적 활동 가능성)에 따라 선제적인 조치를 취하는 등 감사 추적성 확보는 물론 자율적인 운영 체계를 갖춘다.

4.3 네트워크 분리 정책

항목	4.3.1 네트워크 세분화 및 그룹간 이동	
설명	네트워크 세분화는 네트워크를 작은 단위로 나누어 보안을 강화하는 방식으로, 그룹 간 이동을 통해 세분화된 네트워크 간에 안전한 이동을 보장한다. 이는 보안 정책을 세밀하게 적용하고, 필요에 따라 특정 그룹 간의 트래픽 이동을 제어하는 데 사용된다.	
성숙단계	기존	네트워크 세분화 및 이동 통제가 거의 이루어지지 않는가?
		기본적인 경계형 네트워크 모델이 적용되어 있는가?
	초기	시스템 중요도에 따라 네트워크가 분리되어 있는가?
		제한적인 보안 통제를 적용하여 네트워크 간 이동 제어가 가능한가?
	향상	네트워크가 워크로드 별로 세분화되어 보안 정책이 각각 이루어지는가?
		네트워크 그룹 간 이동 시 강력한 접근통제와 인증이 수반되는가?
		네트워크 그룹 간 이동 시 실시간 보안 검사 및 트래픽 이동에 대한 관리가 이루어지는가?
	최적화	그룹 간 이동 시 실시간으로 분석되고 제어되는가?
		재인증 없는 그룹 간 이동이 가능한가?
		실시간 보안 정책 조정을 통한 안전한 그룹 간 이동을 보장하는가?

세부 설명

■ **기존**

✓ **네트워크 세분화 및 이동 통제가 거의 이루어지지 않는가?**

- 단일 네트워크 또는 VLAN 중심의 단순 망 구성으로, 내부 시스템 간 통신은 대부분 자유롭게 허용된다. 실무 환경에서는 서버, PC 등 내부 시스템들이 별다른 제약 없이 서로 통신할 수 있는 환경을 의미하며, 이는 특정 시스템 침해 시 다른 시스템으로의 횡적 이동(Lateral Movement)이 발생할 수 있어 취약점을 보유하고 있는 구조이다.

✓ **기본적인 경계형 네트워크 모델이 적용되어 있는가?**

- 외부와 내부 네트워크 간에는 방화벽을 기준으로 세분화 되어 있다. 외부 공격 방어에 집중하는 전통적인 보안 모델이 적용되어 있다. 그러나 내부 네트워크 간의 세분화나 시스템 간 접근통제는 미흡하여, 내부로 침투한 위협이 확산되는 것을 막기 어렵다.

■ **초기**

✓ **시스템 중요도에 따라 네트워크가 분리되어 있는가?**

- 업무 중요도를 기준으로 VLAN 또는 서브넷 단위의 네트워크가 분리되며, 시스템 간 접속과 이동을 제한하는 기본적인 보안 정책을 적용하기 시작한다. 실무 환경에서는 '기존' 단계의 단순 망 구성에서

발전하여, 중요 시스템(예시: 파일 서버, DB 서버 등)이 위치한 네트워크와 일반 시스템이 위치한 네트워크를 분리하고 기본적인 접근제어를 적용하는 수준을 의미한다.

✓ **제한적인 보안 통제를 적용하여 네트워크 간 이동 제어가 가능한가?**

- 방화벽 또는 보안 시스템의 ACL 정책을 통해 분리된 네트워크 간, 또는 주요 시스템에 대해 네트워크 기반의 제한적인 접근제어를 수행하기 시작한다. 실무 환경에서는 단순히 외부/내부 경계뿐만 아니라, 내부의 중요 시스템 그룹과 다른 시스템 그룹 간의 이동(East-West)에 대해 IP 주소 및 포트 기반의 정적 보안 정책을 적용하여 이동 제어를 시작하는 단계를 의미한다.

■ **향상**

✓ **네트워크가 워크로드 별로 세분화되어 보안 정책이 각각 이루어지는가?**

- 각 서비스 유형, 자산 중요도 등을 기준으로 워크로드 단위의 네트워크 세분화(마이크로 세그멘테이션)를 수행하며, SDN 또는 마이크로 세그멘테이션 시스템 등을 통해 분리한다. 실무 환경에서는 NGFW나 ZTNA 기반의 네트워크 기반 마이크로 세그멘테이션 또는 시스템 자체적인 호스트 방화벽, 호스트 IPS 체계(호스트 기반 마이크로 세그멘테이션)를 구축하여 워크로드별로 세분화하고 각각의 보안 정책을 적용한다. 분리된 네트워크 영역별 정책은 중앙 정책 엔진(SDN 컨트롤러, ZTNA 정책 서버 등)을 통해 관리될 수 있다.

✓ **네트워크 그룹 간 이동 시 강력한 접근통제와 인증이 수반되는가?**

- 세분화된 네트워크 그룹(세그먼트) 간 이동 시 단순 IP/포트 기반 제어를 넘어, 개별 호스트 방화벽 체계, 호스트 IPS 체계 등을 통해 필요한 시스템 단위의 접근통제를 적용한다. 실무 환경에서는 호스트 기반 마이크로 세그멘테이션 시스템 등을 활용하여 조건부 접근통제(예시: DB 간 정해진 포트 통신만 허용하거나, 특정 배치 작업 시간에만 마이그레이션 정책을 적용)를 수행한다. 또한, 네트워크 기준의 ZTNA 시스템과 ICAM과 연동하여 그룹 간 이동 요청 시 사용자와 기기의 신뢰도를 실시간으로 평가하고 필요시 추가 인증(MFA)을 요구하는 등 강력한 통제와 인증이 반영하고 있다.

✓ **네트워크 그룹 간 이동 시 실시간 보안 검사 및 트래픽 이동에 대한 관리가 이루어지는가?**

- 네트워크 그룹 간 트래픽 이동 시 풀 패킷 기반의 기반 검사, NDR, 마이크로세 그멘테이션 정책 등이 적용되어 실시간 보안 검사 및 탐지/대응이 가능하다. 실무 환경에서는 NGFW, NDR, XDR 등을 통해 그룹 간 이동 트래픽에 대한 심층적인 검사를 수행하고, 위협 탐지 시 SIEM/SOAR 등과 연동하여 해당 트래픽을 차단하거나 격리하는 등 실시간 관리가 이루어진다.

■ **초기화**

✓ **그룹 간 이동 시 실시간으로 분석되고 제어되는가?**

- 네트워크 그룹(세그먼트) 간 이동이 발생할 때마다 ML/AI 기반의 트래픽 분석을 실시간으로 수행하여 이상 행동을 탐지한다. 실무 환경에서는 NDR, XDR, SIEM/SOAR 등이 연동되어 이동 트래픽의 위험도를 스코어링하고, 이상 행동이 탐지되면 해당 네트워크 세그먼트를 자동으로 격리하거나 ICAM, ZTNA, 마이크로 세그멘테이션 등과 연동하여 접근권한을 실시간으로 제한하는 등 자율적인 제어 조치를 수행한다.

✓ **재인증 없는 그룹 간 이동이 가능한가?**

- 기존 인증 상태(SSO, 세션 토큰 등)를 유지하면서 네트워크 그룹 간 이동이 가능하며, 이동 중에도 사용자 및 기기의 컨텍스트 기반 위험도 평가와 정책 재검토가 자동화되어 동적으로 수행된다. 실무 환경에서는 ICAM, ZTNA, SIEM/SOAR 시스템 등을 통해 사용자의 신뢰 수준이 지속적으로 높게 유지될 경우, 불필요한 재인증 절차 없이 원활한 그룹 간 이동을 지원하면서도 보안 수준을 유지한다.

✓ **실시간 보안 정책 조정을 통한 안전한 그룹 간 이동을 보장하는가?**

- 온프레미스, 클라우드, 하이브리드 환경 전체에서 보안 정책의 생성, 배포, 조정, 폐기까지 전 과정(라이프사이클)이 자동화되어 있다. 실무 환경에서는 중앙 정책 엔진(ICAM, ZTNA, CNAPP 등)이 정책결정지점(PDP) 역할을 통합적으로 수행하며, 환경 변화나 위협 탐지에 따라 자동으로 정책을 결정한다. 이 결정된 정책은 각 환경별 정책시행지점(PEP)(예시: 온프레미스의 방화벽, 클라우드 환경의 IAM 정책, PAM의 접근제어 정책 등)에 실시간으로 반영되어, 모든 환경에서 일관된 보안 정책의 무결성을 자율적으로 유지한다.

4.4 시스템 보안 및 정책 관리

항목	4.4.1 시스템 환경에 따른 정책 관리	
설명	시스템 환경에 따른 정책 관리는 온프레미스(사내 데이터센터) 환경에서 클라우드 환경으로 전환되면서 보안 정책이 달라져야 하는 상황을 반영한 관리 체계이다. 각 환경에 맞는 보안 정책을 수립하고, 변화하는 환경에 맞춰 정책을 조정한다.	
성숙단계	기존	온프레미스 환경에서 보안 정책을 수립하고 있는가?
		수동으로 보안 정책을 유지·관리하고 있는가?
	초기	클라우드 환경으로 전환하면서 보안 정책을 각각에 맞게 수립하고 있는가?
		정책이 자동으로 적용되는가?
	향상	하이브리드 클라우드 환경으로 전환되면서 실시간으로 보안 정책이 조정되는가?
		환경 변화에 따라 정책이 동적으로 변경 가능한가?
	최적화	보안 위협에 맞춘 자율적인 정책 적용이 가능한가?
		정책 관리가 완전히 자동화되어, 변화하는 환경에서도 일관된 보안 정책을 유지할 수 있는가?

세부 설명

■ **기존**

✓ **온프레미스 환경에서 보안 정책을 수립하고 있는가?**

- 대부분의 보안 정책이 사내 네트워크 환경(온프레미스)을 기준으로 설계되어 있다. 실무 환경에서는 경계 기반 접근제어(예시: 방화벽, IPS)를 중심으로 IP 포트 기반의 정적 정책을 구성하여, 주로 외부로부터의 위협을 방어하는 데 집중한다. 내부 시스템 간 통신에 대한 보안 정책은 미흡한 경우가 많다.

✓ **수동으로 보안 정책을 유지·관리하고 있는가?**

- 시스템 별 정책은 관리자에 의해 수작업으로 적용되며, 자동화나 템플릿 기반 관리는 미흡한 상태이다. 실무 환경에서는 관리자가 개별 방화벽이나 시스템에 직접 접속(예시: CLI, GUI)하여 정책을 설정하는 등 시스템별 개별 관리가 이루어진다. 이로 인해 정책 변경에 시간이 오래 걸리거나, 휴먼 에러가 발생하고, 일부 시스템의 정책이 누락되는 등 일관성이 결여될 수 있다.

■ **초기**

✓ **클라우드 환경으로 전환하면서 보안 정책을 각각에 맞게 수립하고 있는가?**

- 사내 자산(온프레미스) 외에도 클라우드 자산에 대한 보안 정책 수립을 병행한다. 실무 환경에서는 클라우드의 특성을 반영한 요구사항(예시: AWS의 Security Group, Azure의 NSG, NCP의 ACG 등)과 클라우드 IAM 정책을 활용하여, 온프레미스와는 다른 클라우드 환경에 맞는 맞춤형 보안 정책을 새롭게 정의하고 적용하기 시작한다.

✓ **정책이 자동으로 적용되는가?**

- 온프레미스 환경에서는 새로운 시스템(서버) 구성 시, 표준화된 프로세스에 따라 자산 등록, 필수 보안 시스템(에이전트 등) 설치, 모니터링 시스템 연동 등이 반자동 또는 스크립트 기반으로 수행되기 시작한다. 클라우드 환경에서는 IaC(Infrastructure as Code)(예시: Terraform, CloudFormation 등) 또는 정책 템플릿을 통해 자산 생성 시 기본적인 보안 정책(예시: 보안 그룹 규칙 생성 등)이 자동으로 함께 배포된다. 이는 '기존' 단계의 완전 수동 설정 방식에서 벗어나, 정책 적용의 일관성과 속도를 향상시키는 초기 단계의 자동화 수준을 의미한다.

■ **향상**

✓ **하이브리드 클라우드 환경으로 전환되면서 실시간으로 보안 정책이 조정되는가?**

- 온프레미스와 클라우드 자산이 혼합된 환경에서 중앙 통합 정책 관리 플랫폼(예시: ICAM, ZTNA, CNAPP 등)을 통해 모든 환경의 정책을 통합하고 실시간으로 동기화한다. 실무 환경에서는 정책 엔진(예시: IAM, ICAM, ZTNA 등)에서 정의된 정책과 계정/권한 정보가 SCIM 프로토콜 등을 통해 클라우드(예시: AWS IAM, Azure AD)로 실시간 동기화/조정된다. 또한, 사용자가 AWS나 Azure 콘솔에 직접 접근하는 대신, PAM 시스템을 통해 클라우드 환경의 시스템(서버) 접근을 중계하고 통합 관리하여 일관된 보안 정책을 적용할 수 있다.

✓ **환경 변화에 따라 정책이 동적으로 변경 가능한가?**

- 새로운 인프라(예시: IaC로 배포된 신규 VM), 사용자, 위치, 워크로드 등이 감지될 때 해당 환경 변화에 따라 중앙 통합 정책 관리 플랫폼(예시: ICAM, ZTNA, CNAPP 등)에서 정책을 재조정하고 실시간으로 배포한다. 실무 환경에서는 SIEM/SOAR 등 모니터링 시스템이 환경 변화나 위협을 탐지하면, 해당 정보를 정책 엔진으로 전달하여 자동으로 관련 보안 정책(예시: 접근권한, 네트워크 세그먼트)을 동적으로 변경하고, CNAPP, CSPM 등을 통해 설정이 적용되었는지 지속적으로 검증한다.

■ **최적화**

✓ **보안 위협에 맞춘 자율적인 정책 적용이 가능한가?**

- 내부 및 외부의 보안 위협(예시: CTI 연동 정보, 내부 이상 징후) 발생 시, ML/AI가 해당 위협 정보를 자동으로 분석하여 중앙 정책 엔진(ICAM, ZTNA, CNAPP 등)을 통해 실시간으로 정책을 조정하고 배포한다. 실무 환경에서는 XDR, SIEM/SOAR 시스템에서 위협을 탐지하면, 연동된 정책 엔진이 관리자 개입 없이 관련 시스템(예시: PAM, ZTNA, 마이크로 세그멘테이션 등)의 정책을 자율적으로 변경하여 위협을 즉시 차단하거나 격리한다.

✓ **정책 관리가 완전히 자동화되어, 변화하는 환경에서도 일관된 보안 정책을 유지할 수 있는가?**

- 온프레미스, 클라우드, 하이브리드 환경 전체에서 정책의 생성, 배포, 조정, 폐기까지의 전 과정이 라이프사이클 기반으로 관리된다. IaC(Infrastructure as Code) 및 CI/CD 파이프라인을 통해 완전히 자동화된다. 실무 환경에서는 CSPM/CNAPP 솔루션 등이 GitOps 워크플로우와 통합되어, 정책 변경(예시: 코드 커밋) 시 버전 관리, 충돌/중복 검토, 보안성 검증(Scan)을 자동으로 수행하고 배포한다. 이를 통해 변화하는 환경에서도 전사적으로 보안 정책의 무결성과 일관성을 실시간으로 유지한다.

5. 애플리케이션 및 워크로드

5.1 애플리케이션 접근

항목	5.1.1 리소스 권한 부여 및 통합	
설명	응용 및 시스템에 대한 접근권한을 관리하고, 이를 다른 보안 시스템과 통합하여 보안을 강화하는 과정으로, 표준화된 리소스 승인 게이트웨이를 설정하여 관리한다.	
성숙단계	기존	접근에 대한 사용자·시스템 권한을 수동으로 관리하는가?
		리소스에 대한 접근권한을 정의하고, 정적 속성에 기반한 접근제어를 수행하는가?
	초기	워크로드 접근에 대하여 중앙 집중식 관리 시스템이 도입되었는가?
		모든 리소스에 대한 권한을 중앙에서 관리하는가?
	향상	다수의 컨텍스트 정보(위치, 시간 등 포함)을 통한 최소 권한을 부여한 리소스 접근이 가능한가?
		정밀한 권한 관리가 구현되어 이를 통한 리소스 접근이 가능한가?
	최적화	실시간 위험 분석, 행동 패턴 분석 등을 통한 워크로드 및 리소스 접속이 가능한가?
		자동화된 접근권한 부여 및 회수 시스템이 도입되어 있는가?
		실시간 권한 관리 및 비정상적인 접근 차단이 가능한가?
		모든 리소스 권한 부여가 자동화되어 있는가?

세부 설명

■ **기존**

✓ **접근에 대한 사용자·시스템 권한을 수동으로 관리하는가?**

- 애플리케이션 및 워크로드에 대한 권한 부여와 회수 과정이 관리자의 수작업으로 진행된다. 실무 환경에서는 권한 신청을 이메일이나 그룹웨어 결재로 받아서 관리자가 애플리케이션 개발자가 개별 애플리케이션의 관리자 콘솔에 접속하여 수동으로 권한을 적용한다. 이로 인해 정기적인 권한 점검이 어렵고 권한 관리가 누락 되기 쉬운 형태이다.

✓ **리소스에 대한 접근권한을 정의하고, 정적 속성에 기반한 접근제어를 수행하는가?**

- 사용자 역할(Role) 또는 부서 등 정적인 기준으로 리소스 접근제어(RBAC)를 적용한다. 실무 환경에서는 애플리케이션 내에서 '관리자 그룹', '사용자 그룹' 등으로 권한을 분리하는 수준이며, 제로트러스트 원칙에 따라 사용자의 위치, 기기 상태 등 컨텍스트에 따른 동적 권한 제어는 부족하다.

■ **초기**

✓ **워크로드 접근에 대하여 중앙 집중식 관리 시스템이 도입 되었는가?**

- 사용자, 시스템뿐만 아니라 애플리케이션 및 워크로드의 접근권한을 중앙 집중식 관리 시스템(IAM 등)을 통해 일괄적으로 관리하기 시작한다. 실무 환경에서는 식별자 관리에서 중앙화된 계정 정보를 SSO와 연동하여 업무시스템에 해당하는 애플리케이션에 대한 접근을 제어하거나, PAM 시스템과 연동하여 시스템(서버, DB, 쿠버네티스 등)에 대한 접근을 중앙에서 통제하는 단계를 의미한다.

✓ **모든 리소스에 대한 권한을 중앙에서 관리하는가?**

- 실무 환경에서는 '기존' 단계의 개별 애플리케이션, 시스템별 관리를 넘어, 환경별로 중앙 집중화를 시작하는 단계를 의미한다. 예를 들어, 온프레미스 리소스는 사내 IAM 시스템을 통해 계정과 권한 관리를 통합 관리하고, 클라우드 리소스는 각 클라우드 플랫폼(예: AWS, Azure, NCP, NHN 등)의 IAM 기능이나 별도 클라우드 대상 IAM 시스템 등을 통해 해당 플랫폼 내의 권한을 중앙에서 관리한다. 이 단계에서는 아직 전사적인 단일 통합 플랫폼은 부재하며, 각 환경 별 계정과 권한을 중앙 관리하는 수준이다.

■ **향상**

✓ **다수의 컨텍스트 정보(위치, 시간 등 포함)을 통한 최소 권한을 부여한 리소스 접근이 가능한가?**

- 사용자 위치, 기기 보안 상태, 시간대 등의 다수 컨텍스트 정보에 기반한 접근제어(ABAC)를 수행하고, 업무상 필요한 최소한의 권한만을 부여한다. 실무 환경에서는 중앙 정책 엔진(PDP)이 이러한 다수의 컨텍스트 정보를 실시간으로 분석하여 접근 허용 여부를 결정하고, 정책시행지점(PEP)이 이 결정을 받아 애플리케이션 및 워크로드 리소스 접근을 제어한다.

✓ **정밀한 권한 관리가 구현되어 이를 통한 리소스 접근이 가능한가?**

- 정적 RBAC와 컨텍스트 기반 ABAC를 결합하여 유연하면서도 정밀한 권한 모델을 적용한다. 실무 환경에서는 '초기' 단계의 환경별(온프레미스, 클라우드) 분산된 권한 관리에서 확장되어, 중앙 정책결정지점(PDP)(예시: ICAM)에서 전사적인 애플리케이션/리소스에 대한 계정 및 권한 관리가 통합된다. 이 PDP가 사용자의 역할(RBAC)과 속성(ABAC)을 종합하여 접근 결정을 내리면, 이 정보가 각 정책시행지점(PEP)(예시: SSO, PAM 게이트웨이, ZTNA, CASB 등)에 전달되어 실제 리소스 접근을 허용/차단한다.

■ **최적화**

✓ **실시간 위험 분석, 행동 패턴 분석 등을 통한 워크로드 및 리소스 접속이 가능한가?**

- ML/AI 기반의 UEBA 기능이 애플리케이션 및 워크로드 레벨에 적용되어 사용자 행동 및 API 호출 패턴을 실시간으로 분석한다. 실무 환경에서는 CASB(클라우드 앱), WAPP(웹/API), CNAPP(클라우드 네이티브 워크로드) 등이 SIEM/SOAR와 연동되어, 중앙 정책결정지점(PDP)(예시: ICAM)에서 비정상적인 패턴(예시: 과도한 API 요청, 비인가 데이터 접근) 식별 시 동적인 위험 점수를 스코어링하고 접속 여부를 동적으로 결정한다.

✓ **자동화된 접근권한 부여 및 회수 시스템이 도입되어 있는가?**

- ICAM 시스템이 Directory, 그룹웨어, HRM, PAM 등 다양한 시스템과 연동되어, 조직 내 역할 변경, 신청/결재 등 이벤트 발생 시 애플리케이션 및 워크로드에 대한 접근권한을 자동으로 부여/회수한다.

실무 환경에서는 SCIM 프로토콜 등을 통해 퍼블릭 클라우드의 애플리케이션이나 클라우드 워크로드의 계정과 권한까지 라이프사이클 관리가 자동화된다.

✓ **실시간 권한 관리 및 비정상적인 접근 차단이 가능한가?**

- 애플리케이션 및 워크로드 접근 요청 시 ICAM, ZTNA 등 중앙 정책결정지점에서 실시간 위험 점수(사용자/기기 신뢰도, UEBA 분석 결과)를 평가한다. 위협으로 판단되는 경우(예시: CTI 정보와 일치, UEBA 임계치 초과 등), 관리자 개입 없이 정책시행지점(PEP)(예시: CASB, ZTNA 게이트웨이, WAPP 등)을 통해 해당 접근을 자동으로 차단하거나 추가 인증을 요구한다.

✓ **모든 리소스 권한 부여가 자동화되어 있는가?**

- 전사 모든 리소스(온프레미스 애플리케이션, 클라우드 워크로드, SaaS 애플리케이션, API 등)에 대한 권한 부여/회수 프로세스 전반이 JIT(Just-in-Time)/JEA(Just-Enough-Access) 원칙에 따라 완전히 자동화된다. 모든 권한 변경 사항, 접근 시도, 정책결정지점(PDP) 및 정책시행지점(PEP) 로그는 ICAM, SIEM/SOAR 시스템 등으로 통합되고 전송되어 실시간 감사(Audit) 및 모니터링이 가능하다.

5.2 애플리케이션 위협 보호

항목	5.2.1 지속적인 모니터링 및 진행 중인 승인	
설명	자동화된 도구와 프로세스를 사용하여 응용 및 시스템의 보안 상태를 지속적으로 모니터링하고, 실시간으로 보안 승인을 관리하는 과정이다.	
성숙단계	기존	애플리케이션 및 시스템에 대한 보안 상태를 수동으로 모니터링하는가?
		보안 이벤트 기록을 수동으로 수행하는가?
	초기	자동화된 보안 모니터링 도구를 도입하여 실시간으로 보안 이벤트를 수집하고 분석하는가?
		시스템 변경 사항에 대하여 보안 검토를 수행하는가?
	향상	보안 이벤트를 AI 기반으로 분석하고 이상 징후를 탐지하는가?
		보안 승인 프로세스를 자동화할 수 있는가?
	최적화	모든 시스템의 보안 상태를 실시간으로 탐지하고 위협을 사전에 예측할 수 있는가?

세부 설명

■ **기존**

✓ **애플리케이션 및 시스템에 대한 보안 상태를 수동으로 모니터링하는가?**

- 업무 환경에서는 운영자나 개발자가 개별 애플리케이션 서버의 자체 로그 파일이나 관리 콘솔을 통해 애플리케이션 및 시스템 상태를 수동으로 점검한다. 이는 주기적인 확인이나 장애 발생 후 사후 점검 수준에 머무르며, 실시간 위협 탐지나 대응은 불가능한 상태이다.

✓ **보안 이벤트 기록을 수동으로 수행하는가?**

- 보안 이벤트 발생 시 이를 중앙에서 자동으로 수집하거나 기록하는 시스템이 부재하다. 실무 환경에서는 각 애플리케이션에서 발생하는 이벤트를 수동 보고(예시: 이메일 발송, 티켓 발급)하거나, 관리자가 수작업으로 별도의 이벤트를 모아 기록하여 관리한다. 이로 인해 이벤트 기록이 누락 될 가능성이 높고, 통합 분석이 어렵다.

■ **초기**

✓ **자동화된 보안 모니터링 도구를 도입하여 실시간으로 보안 이벤트를 수집하고 분석하는가?**

- 기본적인 SIEM 시스템을 도입하여 애플리케이션(예시: 웹서버, WAS) 로그 및 시스템/DB 로그 등 보안 이벤트를 중앙에서 수집하고, 사전에 정의된 기본 규칙(Rule) 기반의 상관 분석을 수행한다. 실무 환경에서는 '기존' 단계의 수동 로그 점검에서 벗어나, 보안 경보를 실시간으로 기록하고 관리자에게 알림을 전송하는 초기 단계의 자동화된 모니터링 체계를 의미한다.

✓ **시스템 변경 사항에 대하여 보안 검토를 수행하는가?**

- 시스템의 코드나 구성 변경 시 운영 환경에 반영하기 전, 보안 승인을 선행하는 공식적인 절차가 수립되어 있으나, 이 승인 프로세스가 시스템을 통해 자동화되기보다는 주로 수동적인 절차에 의존한다. 실무 환경에서는 개발자의 코드 변경이나 운영자의 서버 설정 변경 요청 시, 보안 담당자가 보안성 심의나 보안성 검토를 통해 이를 수동으로 검토하고 승인하는 절차를 운영하는 수준을 의미한다. 추가적으로 기본적인 SIEM 시스템을 도입하여 애플리케이션(예시: 웹서버, WAS) 로그 및 시스템/DB 로그 등 보안 이벤트를 중앙에서 수집하고, 사전에 정의된 기본 규칙(Rule) 기반의 상관 분석을 수행한다. 이는 수동 로그 점검에서 벗어나, 보안 경보를 실시간으로 기록하고 관리자에게 알림(예시: 이메일, 메신저)을 전송하는 초기 단계의 자동화된 모니터링 체계를 구축하기 시작한 단계이다.

■ **향상**

✓ **보안 이벤트를 AI 기반으로 분석하고 이상 징후를 탐지하는가?**

- 기존의 규칙 기반 탐지에서 확장되어, ML/AI 기반의 사용자 별 UEBA 기능이 도입되어 애플리케이션과 시스템의 동작 패턴을 분석한다. SIEM이나 XDR 솔루션에 탑재된 ML/AI 엔진이 사용자(예시: 개발자, 운영자) 및 시스템(예시: WAS, DB 서버)의 정상적인 활동 기준선(Baseline)을 학습한다. 이후, 평소와 다른 비정상적인 API 호출, 과도한 데이터 조회, 권한 상승 시도 등 알려지지 않은 위협이나 내부자 위협 징후를 실시간으로 탐지하여 경보를 발생시킨다.

✓ **보안 승인 프로세스를 자동화할 수 있는가?**

- 애플리케이션 배포나 시스템 설정 변경 시, 보안 검토 및 승인 프로세스가 자동화된다. DevSecOps 파이프라인과 연계되어, 코드 변경(Commit) 시 정의되어 있는 보안성 검토 절차에 맞게 SAST/DAST/SCA 시스템과 연동되어 자동으로 보안성 검토 수행하고, 이 검사 결과를 바탕으로 위험 수준(예시: Critical 취약점 0개)에 따라 자동으로 운영 환경 배포를 승인하거나 거절(차단)하는 등, 보안 승인 절차가 워크플로우에 통합되어 자동화된 것을 의미한다.

■ **최적화**

✓ **모든 시스템의 보안 상태를 실시간으로 탐지하고 위협을 사전에 예측할 수 있는가?**

- 모든 애플리케이션과 워크로드의 보안 상태를 실시간으로 모니터링하는 기능을 포함하여, 지속적인 보안 모니터링과 ML/AI 기반 위협 예측 기능이 통합되어 잠재적인 공격 시나리오를 사전에 차단한다. 실무 환경에서는 XDR, CNAPP, SIEM/SOAR 등의 시스템이 유기적으로 통합되어, 외부 위협 인텔리전스(CTI), 내부 시스템 로그, 애플리케이션 트래픽, 사용자 행위 등 방대한 데이터를 AI 엔진이 지속적으로 학습하고 분석한다. 이를 통해 개별 이상 징후 탐지를 넘어, 여러 징후를 조합하여 '잠재적인 다단계 공격 시나리오'를 사전에 예측하고, 관련 시스템의 보안 태세(예시: 접근권한, 네트워크 정책)를 자동으로 강화하거나 선제적으로 차단 조치를 수행한다. 이러한 모든 보안 상태 평가는 자동화되어 애플리케이션 및 시스템의 정책에 지속적으로 반영되는 등 자율적인 보안 상태 관리가 이루어진다.

5.3 접근 가능한 애플리케이션

항목	5.3.1 원격 접속	
설명	사용자가 외부에서 안전하게 조직의 네트워크에 접속할 수 있도록 하는 보안 조치이다. 최소 권한 기준을 설정하기 위해 기존 장치 접근 프로세스 및 도구를 사용한다. 승인된 응용에 대해 Enterprise IDP를 사용하는 디바이스 및 IoT 등이 원격 접속 지원을 포함하도록 확장한다.	
성숙단계	기존	VPN을 통해서 외부 접속을 지원하는가?
		애플리케이션에 대한 접근제어가 제한적인가?
	초기	원격 접속 기기의 보안 상태를 자동으로 평가하고 접근을 제어하는가?
		원격 접속 기기의 실시간 모니터링 및 제어가 가능한가?
	향상	다양한 원격 접속 시나리오에 대한 맞춤형 보안 정책을 수립하였는가?
		접속 상황에 따라 동적 보안 정책을 적용하여 애플리케이션 기능이 필요시 제한하는가?
	최적화	AI를 활용하여 원격 접속 보안을 고도화하였는가?
		AI를 통하여 위험 요소가 탐지되면 애플리케이션 기능이 즉각적으로 제한 또는 차단되는가?

세부 설명

■ **기존**

✓ **VPN을 통해서 외부 접속을 지원하는가?**

- 전통적인 경계 기반 보안 모델에 의존하여, 외부에서의 원격 접속은 주로 방화벽이나 SSL-VPN 시스템 등을 통해 이루어진다. 실무 환경에서는 사용자가 VPN 터널링을 통해 암호화된 세션을 맺고 내부 네트워크(LAN)에 일단 접속하면, 해당 네트워크 대역에 대한 접근권한을 일괄적으로 부여받는다. 이로 인해, 원격 접속 후 내부망에서 접근할 수 있는 애플리케이션에 대한 세분화된 접근제어가 제한적이며 (예시: VPN 접속에 성공하면 내부의 모든 애플리케이션에 원칙적으로 접근 가능), 최소 권한 원칙 준수가 미흡한 상태이다.

✓ **애플리케이션에 대한 접근제어가 제한적인가?**

- SSL-VPN 등을 통해 VPN 터널링이 연결되면, 사용자는 정해진 애플리케이션(예시: 특정 업무시스템, 그룹웨어 등)에 대한 접근을 수행한다. 하지만, 접속이 허용된 이후에는 해당 애플리케이션이 속한 내부 IP 대역(네트워크 세그먼트)별 세부적인 정책이 부여되지 않아 횡적 이동(Lateral Movement)의 위협이 존재하며 최소 권한 제어가 미흡한 상태이다.

■ **초기**

✓ **원격 접속 기기의 보안 상태를 자동으로 평가하고 접근을 제어하는가?**

- 원격 접속 기기의 보안 상태를 자동으로 평가하고 접근을 제어하기 시작한다. 실무 환경에서는 외부에서 내부로 접근 시, NAC, EDR, AV(백신), NGFW, SASE 등의 시스템을 통해 해당 기기의 보안 상태(예시: 백신/AV 설치 여부, OS 최신 패치 적용 여부, 필수 보안 S/W 설치 여부 등)를 자동으로 평가한다. 이 평가 결과, 조직의 보안 기준에 부합하는 경우에만 내부 접근을 허용하고, 기준 미달 시에는 접속을 제한하거나 격리 네트워크로 유도하는 등 초기 수준의 조건부 접근제어를 수행한다.

■ **향상**

✓ **원격 접속 기기의 실시간 모니터링 및 제어가 가능한가?**

- SASE/ZTNA 게이트웨이나 NGFW 시스템 등을 통해 원격 접속 중인 기기의 상태 변화(예시: 위협 감지, 보안 설정 변경, 비인가 S/W 설치)를 실시간으로 모니터링하고 제어한다. 실무 환경에서는 AV, EDR, NAC 등과 NGFW, ZTNA 시스템을 연동하거나 ZTNA 시스템 자체적으로, 기기에서 위협이 탐지되는 즉시 해당 기기의 IP나 세션 정보를 정책 엔진으로 전달받아, 관리자 개입 없이도 네트워크 접근을 동적으로 차단하거나 격리하는 등 즉각적인 세션 제어가 이루어진다.

✓ **다양한 원격 접속 시나리오에 대한 맞춤형 보안 정책을 수립하였는가?**

- 조직의 환경에 맞게 다양한 원격 접속 시나리오별로 맞춤형 보안 정책을 수립하고 적용한다. 실무 환경에서는 ICAM, ZTNA, SASE 등의 정책 엔진을 통해 사용자 역할, 기기 상태뿐만 아니라 다양한 컨텍스트를 조합하여 정책을 수립한다. (예시: '국내' 접속 시에는 MFA 인증 후 대부분의 앱을 허용하지만, '해외' IP로 접속 시에는 민감한 시스템 접근을 차단함 / '업무 시간' 외에는 관리자 승인을 요구함 / '회사 노트북'은 모든 접근을 허용하되, '개인 모바일' 기기로는 이메일과 그룹웨어만 허용함)

■ **최적화**

✓ **접속 상황에 따라 동적 보안 정책을 적용하여 애플리케이션 기능이 필요시 제한하는가?**

- 원격 접속 시 애플리케이션 접근 허용 여부를 넘어, 애플리케이션 내부의 세부 기능 단위(예시: 특정 메뉴, 조회 버튼, 다운로드 버튼)까지 접근을 제어하며, 이 권한은 사용자의 실시간 컨텍스트를 기반으로 동적으로 적용된다. 실무 환경에서는 중앙 정책 엔진(PDP) 역할을 수행하는 ICAM이 SIEM/SOAR 등에서 수집·분석된 로그 결과(예시: 사용자 행위, 기기 상태)를 기반으로 사용자의 위험 점수를 실시간으로 스코어링한다. 이 점수에 따라 ICAM이 '조회' 버튼은 허용하되 '다운로드' 버튼은 비활성화하는 등 세부 기능 단위의 동적 보안 정책을 결정하면, SSO, ZTNA, CASB, 마이크로 세그멘테이션 등 실제 접근을 수행하는 정책시행지점(PEP)이 이 정책을 받아 정교한 동적 접근제어를 수행한다.

✓ **AI를 활용하여 원격 접속 보안을 고도화 하였는가?**

- ML/AI 기반의 UEBA 기능이 원격 접속 보안에 적용되어, 사용자의 정상/이상 활동을 실시간으로 판단하고 동적인 위험 점수를 산출하여 적용한다. 실무 환경에서는 SIEM, XDR, ZTNA 시스템 등이 연동되어, AI 엔진이 사용자의 접속 시간, 위치, 기기 상태, 앱 사용 행위 등 다양한 컨텍스트를 종합적으로 분석한다. 이 위험 점수는 정책 엔진(PDP)인 ICAM에 실시간으로 전달되어, 원격 접속 관련 보안 정책(예시: 인증 강도 상향, 접근 가능 권한 축소)을 자동으로 조정하는 등 고도화된 보안 체계를 운영한다.

✓ **AI를 통하여 위험 요소가 탐지되면 애플리케이션 기능이 즉각적으로 제한 또는 차단되는가?**

- ML/AI 엔진이 UEBA 분석이나 CTI 연동 등을 통해 실제 보안 위협(예시: 비정상적인 대량 데이터 접근, 내부 확산 시도)이나 고위험 요소를 실시간으로 탐지하면, 이 정보가 SIEM/SOAR 시스템 등과 연동되어 관리자 개입 없이 즉각적인 자동 대응을 수행한다. 실무 환경에서는 SOAR 플레이북이 실행되어, 탐지된 위협의 심각도에 따라 정책시행지점(PEP)(예시: ZTNA, CASB, 마이크로 세그멘테이션 등)을 통해 해당 사용자의 특정 애플리케이션 기능을 즉시 중단시키거나, 세션을 강제 격리/종료하고, MFA 재인증을 요구하는 등 자율적인 보안 조치가 자동으로 이루어진다.

5.4 안전한 애플리케이션 배포

항목	5.4.1 안전한 애플리케이션 배포	
설명	안전한 응용 배포란 응용을 배포할 때 발생할 수 있는 보안 위협을 최소화하기 위한 프로세스와 도구를 사용하는 것을 의미한다. 이는 보안 정책 준수, 취약점 검사, 자동화된 배포 파이프라인, 코드 무결성 검증, 환경 격리 및 모니터링을 포함한다.	
성숙단계	기존	애플리케이션 배포 전 수동으로 코드 검토 및 취약점 검사를 수행하는가?
		보안 가이드라인을 준수하는 초기 배포 절차를 마련하였는가?
		기본적인 배포 접근제어를 적용하여 배포 과정에서의 보안 사고를 방지하고 있는가?
	초기	보안이 내재된 자동화된 배포 파이프라인을 구축하였는가?
		애플리케이션 배포 시 보안이 자동으로 적용되는가?
		CI/CD 파이프라인을 통하여 자동화된 취약점 검사 도구를 적용하였는가?
		배포 전후로 코드 무결성을 검사하고 배포 환경을 격리하였는가?
	향상	배포 과정 전반에 걸쳐 지속적인 모니터링을 수행하는가?
		보안 정책 준수를 자동으로 검증하는 도구가 도입되어 있는가?
		배포 중 발생하는 비정상적인 활동을 모니터링하여 즉각 대응 가능한가?
		애플리케이션의 모든 구성요소가 배포 전후로 보안 검사를 거치도록 구성하였는가?
	최적화	완전히 자동화된 코드 배포 및 관리자 권한 접근제어가 가능한가?
		AI를 활용한 고도화된 위협 탐지 및 대응 시스템을 배포 파이프라인에 통합하여 중앙에서 관리하고 자동 보고 및 추적 관리가 가능한가?

세부 설명

■ **기존**

✓ **애플리케이션 배포 전 수동으로 코드 검토 및 취약점 검사를 수행하는가?**

- 애플리케이션 배포 전 보안성 검토가 SDLC(소프트웨어 개발 생명주기)에 체계적으로 통합되어 있지 않으며, 주로 개발자가 자체적으로 시큐어 코딩 점검을 수행한다. 애플리케이션을 배포하거나 상품화하는 최종 단계나, 1년 기준의 주기적인 취약성 검토 수준에서만 취약점 점검 도구 등을 활용해 수동으로 코드 검토 및 취약점 점검을 수행한다.

✓ **보안 가이드라인을 준수하는 초기 배포 절차를 마련하였는가?**

- 조직의 컴플라이언스 기준(예시: OWASP Top 10)에 따른 기본적인 소프트웨어 개발 보안 가이드라인이나 표준 운영 지침이 문서로 수립되어 있다. 하지만 이 가이드라인이 CI/CD 파이프라인 등에 자동화되어 강제되지 않고, 배포 시 개발자나 운영자가 매뉴얼(체크리스트)을 통해 준수 여부를 검토하는 수준에 머무른다.

✓ **기본적인 배포 접근제어를 적용하여 배포 과정에서의 보안 사고를 방지하고 있는가?**

- CI/CD 도구나 배포 대상 시스템(예시: 운영 서버)에 접근하는 계정에 대해 기본적인 접근제어 정책을 적용한다. 실무 환경에서는 Directory 그룹 등을 활용하여 배포 권한을 정적인 방식으로 일괄 부여하며, 개발자와 운영자 간의 역할 분리가 명확하지 않거나 최소 권한 원칙이 엄격하게 적용되지 않은 상태이다.

■ **초기**

✓ **보안이 내재된 자동화된 배포 파이프라인을 구축하였는가?**

- SDLC(소프트웨어 개발 생명주기)가 명확히 정의되어, '보안이 내재된 소프트웨어 배포' 개념을 도입하기 시작한다. 실무 환경에서는 CI/CD 파이프라인에 빌드부터 배포까지의 단계를 정의하며, 이 과정에 보안 점검을 포함시키는 초기 DevSecOps 체계를 구축하기 시작한다.

✓ **애플리케이션 배포 시 보안이 자동으로 적용되는가?**

- CI/CD 파이프라인의 CI(Continuous Integration) 단계에서 보안 검사가 자동으로 적용되기 시작한다. 실무 환경에서는 개발자가 코드를 커밋할 때, SAST(정적 분석)를 자동으로 실행하여 시큐어 코딩 규칙 위반 여부를 검사하고, 보안 문제가 발견되면 빌드를 중단시키는 등 SDLC에 보안을 내재화하는 초기 DevSecOps 체계를 구축한다.

✓ **CI/CD 파이프라인을 통하여 자동화된 취약점 검사 도구를 적용하였는가?**

- 자동화된 취약점 검사 도구(예시: SAST, SCA)를 CI/CD 파이프라인에 적용한다. 실무 환경에서는 CI 단계에서 SCA 도구가 자동으로 실행되어 알려진 취약점(CVE)이 있는 오픈소스 라이브러리를 탐지하거나, SAST 도구가 코드 레벨의 취약점을 탐지하고, 그 결과를 개발자에게 자동 리포트한다. DAST는 테스트 환경 배포 후 제한적으로 적용된다.

✓ **배포 전후로 코드 무결성을 검사하고 배포 환경을 격리하였는가?**

- 배포될 산출물의 무결성을 검증하고, 배포 환경을 격리하기 시작한다. 실무 환경에서는 코드 서명이나 해시(Hash)값 비교를 통해 빌드된 아티팩트(Artifact)의 변경 유무(무결성)를 검사한다. 또한, 개발 환경, 테스트 환경, 운영 환경을 별도의 네트워크 세그먼트나 VLAN으로 분리하여, 배포가 격리된 환경에서 안전하게 실행되도록 구성한다.

■ **향상**

✓ **배포 과정 전반에 걸쳐 지속적인 모니터링을 수행하는가?**

- 전사적인 애플리케이션 배포가 SDLC(소프트웨어 개발 생명주기) 내에서 관리되며, 배포 과정 전반에 걸쳐 지속적인 모니터링이 이루어진다. 실무 환경에서는 CI/CD 파이프라인에서 발생하는 모든 로그(예시: 빌드 시작, 테스트 실패, 배포 승인/거절) 및 배포 대상 시스템의 이벤트 로그를 SIEM으로 실시간 전송하여 중앙에서 통합 모니터링한다. 이를 통해 배포 과정에서 발생하는 보안 이벤트(예시: 허가되지 않은 이미지 사용, 승인되지 않은 코드 변경 시도)를 실시간으로 탐지하고 위협 분석을 수행하여 조치를 진행한다.

✓ **보안 정책 준수를 자동으로 검증하는 도구가 도입되어 있는가?**

- SDLC의 배포 단계(CD)에 보안 정책을 자동으로 검증하는 도구가 도입된다. 실무 환경에서는 CI/CD 파이프라인 내에 '보안 게이트' 등을 설정하여, 사전에 정의된 보안 정책(예시: SAST/DAST 검사 통과 여부, 오픈소스 취약점(SCA) 임계치 미만, 컨테이너 이미지 서명 검증 등)에 부합하지 않으면 배포를 자동으로 차단하거나 롤백하도록 설정된 검증 모듈이 작동한다.

✓ **배포 중 발생하는 비정상적인 활동을 모니터링하여 즉각 대응 가능한가?**

- 배포 과정 중 발생하는 사용자 및 시스템의 비정상적인 활동을 실시간으로 탐지하고 즉각적인 대응을 수행한다. 실무 환경에서는 배포 권한을 가진 계정의 평소와 다른 활동(예시: 업무 시간 외 배포 시도, 과도한 권한으로 빌드 서버 접근, 배포 대상 시스템 변조 시도)을 SIEM, UEBA, PAM 등의 시스템을 통해 실시간으로 탐지한다. 탐지 시, SIEM/SOAR와 연동하여 관리자에게 자동으로 알림을 보내거나 관련 계정을 즉시 비활성화하고, 배포 프로세스를 강제 중단하는 등의 즉각적인 대응이 이루어진다.

✓ **애플리케이션의 모든 구성 요소가 배포 전후로 보안 검사를 거치도록 구성 하였는가?**

- 전사적인 애플리케이션 배포가 SDLC 내에서 관리되며, 애플리케이션을 구성하는 모든 요소가 배포 전후로 보안 검사를 거치도록 구성된다. 실무 환경에서는 전체 애플리케이션 아키텍처에 포함된 마이크로서비스, API, 외부 라이브러리(SCA), 컨테이너 이미지 등이 CI/CD 파이프라인의 각 단계에서 개별적으로 보안 검사(SAST, DAST, IAST 등)를 수행한다. 이 모든 검증 절차를 통과하여 보안 인증이 완료된 구성 요소(아티팩트)만이 최종적으로 운영 환경에 배포된다.

■ **최적화**

✓ **완전히 자동화된 코드 배포 및 관리자 권한 접근제어가 가능한가?**

- IaC(Infrastructure as Code)를 기반으로, 인프라 구성과 애플리케이션 배포가 완전히 자동화된 단계이다. 실무 환경에서는 GitOps 워크플로우 등과 통합되어, 코드 커밋(Commit)을 통해 모든 변경 사항(예시: 인프라 설정, 애플리케이션 업데이트)이 자동으로 검증되고 배포된다. 이 과정에서 운영 서버나 CI/CD 파이프라인에 대한 관리자의 직접적인 접근은 원천적으로 차단되며, 배포는 사전에 정의된 최소 권한의 서비스 계정을 통해서만 실행된다. 긴급 장애 대응 등 예외적인 관리자 접근이 필요할 경우, 마이크로 세그멘테이션, PAM 시스템 등과 연동하여 JIT/JEA 원칙에 따라 필요한 시간 동안만 최소한의 명령어 실행 권한을 동적으로 부여받는다.

✓ **AI를 활용한 고도화된 위협 탐지 및 대응 시스템을 배포 파이프라인에 통합하여 중앙에서 관리하고 자동 보고 및 추적 관리가 가능한가?**

- CI/CD 파이프라인 전반에 ML/AI 기반의 위협 탐지 및 대응 시스템이 완전히 통합되어, 중앙에서 자율적인 관리가 이루어진다. 실무 환경에서는 ML/AI 엔진이 배포 과정의 로그, 개발자의 행위 패턴(예시: 평소와 다른 코드 커밋 시간, 비정상적인 빌드 서버 접근 시도), 외부 위협 인텔리전스(CTI) 정보 등을 실시간으로 분석하여 고도화된 위험 요소를 탐지한다. 탐지된 위협은 즉시 SIEM/SOAR 시스템과 연동되어, 관리자 개입 없이도 자동화된 플레이북을 통해 배포를 즉각 중단시키거나, 관련 계정을 격리/차단하는 등 자동화된 대응이 수행된다. 모든 배포 및 보안 검증 결과, 대응 이력은 중앙화된 단일 플랫폼(예시: ICAM, 정보보안 포털)에서 자동으로 보고되며, 완전한 감사 추적성이 보장된다.

항목	5.4.2 애플리케이션 인벤토리	
설명	조직 내에서 사용되는 모든 응용을 식별하고, 이를 체계적으로 관리하는 과정이다. 인벤토리를 통해 응용의 상태, 소유권, 사용 목적 등을 파악할 수 있다.	
성숙단계	기존	모든 애플리케이션의 인벤토리를 수동으로 목록화하였는가?
		애플리케이션 기본 정보를 기록하여 관리하는가?
	초기	자동화된 인벤토리 도구를 도입하여 애플리케이션을 자동으로 식별하고 관리할 수 있는가?
	향상	애플리케이션 인벤토리에 보안 정보를 추가하여 애플리케이션의 보안 상태를 평가·관리할 수 있는가?
	최적화	AI 기반 인벤토리 관리 시스템을 도입하여 애플리케이션 변경 사항을 실시간으로 반영할 수 있는가?
		애플리케이션 인벤토리를 다른 보안 시스템과 통합, 종합적인 보안 관리가 이루어지고 있는가?

세부 설명

■ 기존

✓ **모든 애플리케이션의 인벤토리를 수동으로 목록화하였는가?**

- 조직 내부에서 개발하거나 업무시스템으로 사용되는 모든 애플리케이션을 식별하여 스프레드시트 등을 활용해 수작업으로 목록(인벤토리)을 작성하여 관리한다. 실무 환경에서는 각 애플리케이션별로 담당자(개발자/운영자/관리자 등)가 배정되어 관리되고 있는 상태를 의미한다.

✓ **애플리케이션 기본 정보를 기록하여 관리하는가?**

- 애플리케이션의 기본 정보(예시: 이름, 버전, 담당자, 서버 위치 등)를 기록하여 목록을 관리한다. 또한, 애플리케이션의 종류 및 활용 목적(예시: 대외 서비스, 내부 업무용, 개발용 등)에 따라 자산을 분류하고, 이 분류된 기준에 따라 기본적인 보안 정책(예시: 대외 서비스는 웹 방화벽 기능 적용, 내부 시스템은 사내망 접근만 허용 등)을 정의하여 관리하는 수준을 의미한다.

■ 초기

✓ **자동화된 인벤토리 도구를 도입하여 애플리케이션을 자동으로 식별하고 관리할 수 있는가?**

- 자산관리시스템(ITAM)이나 별도의 그룹웨어 등을 통해 애플리케이션 인벤토리를 관리하기 시작한다. 실무 환경에서는 네트워크 스캔, 에이전트 기반 또는 API 연동 방식을 바탕으로 설치되어 있는 애플리케이션을 자동으로 탐지하고, 식별된 정보를 ITAM이나 그룹웨어의 인벤토리에 주기적으로 갱신한다. 또한, 개발 소스코드 관리를 위해 사용하는 깃허브(GitHub) 등의 형상 관리 도구를 애플리케이션 인벤토리 관리의 일부로 통합하여 활용할 수도 있다.

■ 향상

✓ **애플리케이션 인벤토리에 보안 정보를 추가하여 애플리케이션의 보안 상태를 평가·관리할 수 있는가?**

- 식별된 애플리케이션 인벤토리에 다양한 보안 관련 정보를 통합하여 관리하는 단계이다. 실무 환경에서는 DevSecOps 파이프라인과 연계하여, CI/CD 과정에서 수행된 SAST/DAST/SCA 검사 결과(예시: 탐지된 취약점 목록, CVE 번호), SBOM(소프트웨어 구성요소 명세서) 정보, 패치 상태, 사용된 인증서 유효성, 애플리케이션이 보유한 접근권한(예시: API 키, DB 접근 계정) 등의 보안 정보를 인벤토리에 자동으로 추가하고 매핑한다. 이를 통해 관리자는 단순히 애플리케이션 목록을 넘어, 각 애플리케이션의 현재 보안 상태와 위험도를 지속적으로 평가하고 관리한다.

■ 최적화

✓ **AI 기반 인벤토리 관리 시스템을 도입하여 애플리케이션 변경 사항을 실시간으로 반영할 수 있는가?**

- ML/AI 기반의 인벤토리 관리 시스템을 도입하여 애플리케이션의 변경 사항을 실시간으로 반영한다. 실무 환경에서는 클라우드 네이티브 환경(예시: 쿠버네티스)에서의 오토스케일링이나 신규 배포로 인해 수시로 변경되는 애플리케이션 및 워크로드의 설치/변경/삭제 이벤트를 ML/AI 기반 이상 탐지 또는 실시간 로그 분석을 바탕으로 자동으로 감지한다. 감지된 내용은 즉시 애플리케이션 인벤토리에 실시간으로 반영되어 항상 최신 상태를 유지한다.

✓ **애플리케이션 인벤토리를 다른 보안 시스템과 통합, 종합적인 보안 관리가 이루어지고 있는가?**

- '향상' 단계에서 확보된 인벤토리의 보안 정보(예시: 취약점 상태, SBOM, 권한)가 다른 보안 시스템과 유기적으로 통합되어 종합적인 보안 관리가 이루어진다. 실무 환경에서는 인벤토리 데이터가 중앙 정책 엔진(PDP)(예시: ICAM) 및 SIEM/SOAR, ZTNA, CNAPP 등과 실시간으로 연동된다. 이를 통해 정책 엔진은 애플리케이션의 최신 보안 상태(예시: 심각한 취약점(CVE)이 발견된 앱)를 접근제어 정책에 동적으로 반영할 수 있으며, SIEM/SOAR 시스템에서 위협 탐지 및 통합 대응(예시: '취약한 앱'이 설치된 기기 자동 격리)에 인벤토리 정보를 활용하는 등 완전 자동화된 정책 적용 및 위협 대응이 수행된다.

5.5 소프트웨어·애플리케이션 보안

항목	5.5.1 안전한 소프트웨어 개발 및 통합	
설명	소프트웨어 개발 라이프사이클(SDLC) 전반에 걸쳐 보안 요소를 내제화학, 개발된 소프트웨어를 안전하게 통합하는 과정이다. 코드 검토, 런타임 보호, 보안 API 게이트웨이, 컨테이너 및 서버리스 보안과 같은 제어 기능이 통합되고 자동화된다. DevSecOps를 통하여 워크플로우를 구성한다.	
성숙단계	기존	개발 프로세스에 보안 코딩 표준이 적용되어 있는가?
		코드 배포 전, 정적이고 수동으로 보안 테스트를 수행하는가?
	초기	보안 검토와 테스트를 소프트웨어 개발 라이프사이클에 통합하여 개발 단계부터 보안 취약점을 식별하는가?
		DevSecOps 문화를 도입하였는가?
		주요 개발 내용에 대한 SBOM 문서를 작성하는가?
	향상	서드파티 라이브러리 및 오픈소스 소프트웨어의 보안 검사를 자동화하여 수행하는가?
		프로세스 전반에 걸친 SBOM 문서를 작성하는가?
	최적화	소프트웨어 개발과 관련된 조직의 프로세스가 격리되어 있는가?
		런타임 소프트웨어에 대한 분석이 자동화되어 있는가?

세부 설명

■ **기존**

✓ **개발 프로세스에 보안 코딩 표준이 적용되어 있는가?**

- 조직의 컴플라이언스 기준(예시: OWASP Top 10, KISA 시큐어코딩 가이드)에 따른 기본적인 소프트웨어 개발 보안 가이드라인이 문서로 수립되어 있다. 실무 환경에서는 이 가이드라인이 개발 프로세스나 SDLC(소프트웨어 개발 생명주기)에 체계적으로 통합되거나 강제되지는 않으며, 주로 개발자에게 교육 자료로 제공되거나 자체적인 점검 용도로 활용되는 수준에 머무른다.

✓ **코드 배포 전, 정적이고 수동으로 보안 테스트를 수행하는가?**

- 애플리케이션 배포 전 보안성 검토가 SDLC에 체계적으로 통합되어 있지 않으며, 정적 분석 도구(SAST) 등을 활용한 보안 테스트가 자동화되지 않은 상태이다. 실무 환경에서는 개발 완료 후 배포 전이나, 1년 단위의 취약점 점검 등 정해진 주기에 따라 보안 담당자가 수동으로 SAST 도구를 실행하여 취약점을 점검하거나, 매뉴얼 방식으로 코드 검토를 수행하는 등 제한적인 수준의 보안 테스트가 이루어진다.

■ **초기**

✓ **보안 검토와 테스트를 소프트웨어 개발 라이프사이클에 통합하여 개발 단계부터 보안 취약점을 식별하는가?**

- SDLC(소프트웨어 개발 생명주기)가 명확히 정의되고, '보안이 내재된 개발' 개념을 도입하기 시작한다.

실무 환경에서는 SDLC의 '개발' 및 '테스트' 단계에 보안 검토와 테스트 활동이 공식적으로 통합된다. (예시: 개발자가 코드를 작성하는 단계에서부터 SAST(정적 분석)를 수행하여 시큐어 코딩 규칙 위반 여부를 검사하고, 테스트 단계에서 DAST(동적 분석)를 통해 기본적인 취약점을 식별하는 등) 개발 초기부터 보안 취약점을 식별하고 수정하는 프로세스를 갖추기 시작한다.

✓ **DevSecOps 문화를 도입하였는가?**

- 보안팀, 개발팀, 운영팀 간의 협업 체계를 수립하고, CI/CD 파이프라인에 보안을 통합하려는 초기 DevSecOps 문화를 도입하기 시작한다. 실무 환경에서는 보안팀이 개발 프로세스에 참여하여 보안 요구사항을 전달하고, 개발팀은 CI 파이프라인에 SAST(정적 분석) 검사를 연동하여 빌드 시 자동으로 실행하는 등, 개발(Dev), 보안(Sec), 운영(Ops)이 함께 보안을 책임지는 문화를 구축하기 시작하는 단계이다.

✓ **주요 개발 내용에 대한 SBOM 문서를 작성하는가?**

- 소프트웨어 공급망 보안의 중요성을 인식하고, 주요 개발 내용에 대한 SBOM(소프트웨어 구성요소 명세서) 작성을 시작한다. 실무 환경에서는 SCA(소프트웨어 구성요소 분석) 도구 등을 도입하여, 빌드 시 애플리케이션에 포함된 오픈소스 라이브러리 및 서드파티 구성요소를 식별하고, 이 목록을 기반으로 SBOM 문서를 수동 또는 반자동으로 생성하여 관리한다. 이는 향후 발견될 취약점에 대비하여 구성요소를 추적할 수 있는 기반을 마련하는 단계이다.

■ **향상**

✓ **서드파티 라이브러리 및 오픈소스 소프트웨어의 보안 검사를 자동화하여 수행하는가?**

- 소프트웨어 공급망 보안을 강화하기 위해, 소스 코드에 포함된 서드파티 라이브러리나 오픈소스 컴포넌트를 자동으로 식별하고, 알려진 취약점(CVE)을 분석 및 경고 처리한다. 실무 환경에서는 SCA(소프트웨어 구성요소 분석) 도구가 CI/CD 파이프라인에 통합되어, 빌드 시점마다 자동으로 실행된다. (예시: 'High' 등급 이상의 CVE가 포함된 오픈소스 라이브러리가 탐지될 경우, 빌드를 실패(Fail) 처리하거나 보안팀에 즉시 경고를 전송하여 조치)

✓ **프로세스 전반에 걸친 SBOM 문서를 작성하는가?**

- '초기' 단계의 수동/반자동 작성을 넘어, SDLC 프로세스 전반에 걸쳐 SBOM 작성을 자동화한다. 실무 환경에서는 SCA 도구나 빌드 도구가 CI/CD 파이프라인과 연동되어, 컴파일 시점 또는 배포 시점마다 최종 배포물(아티팩트)에 포함된 모든 구성요소(라이브러리, 모듈, 의존성 등)의 목록과 버전, 라이선스 정보가 포함된 SBOM이 자동으로 생성되고 저장(예시: 아티팩트 저장소)된다.

■ **최적화**

✓ **소프트웨어 개발과 관련된 조직의 프로세스가 격리되어 있는가?**

- 소프트웨어 개발과 관련된 조직의 프로세스가 물리적·논리적으로 완벽히 격리된다. 실무 환경에서는 '개발', '테스트', '운영' 환경이 ZTNA, 마이크로 세그멘테이션 시스템 등을 통해 네트워크 수준에서 엄격히 분리된다. 또한, CI/CD 파이프라인(예시: Jenkins, GitLab CI) 자체도 격리된 전용 세그먼트에서 실행되며, 각 단계(빌드, 테스트, 배포)는 최소 권한의 서비스 계정으로만 동작한다. 개발자나 운영자의 직접적인 운영 환경 접근은 원천적으로 차단되며, 긴급 접근이 필요할 경우 PAM 시스템과 연동된 JIT(Just-in-Time) 권한 승인을 통해서만 제한적으로 허용된다.

✓ **런타임 소프트웨어에 대한 분석이 자동화되어 있는가?**

- 런타임(Runtime) 환경의 소프트웨어에 대한 분석 및 보호가 자동화된다. 실무 환경에서는 SASE, WAAP, IAST, RASP 시스템 등을 통해, 실제 운영 환경에서 실행 중인 애플리케이션의 내부 동작(예시: 비정상적인 함수 호출, 메모리 접근)이나 API 요청을 지속적으로 모니터링한다. 특히 클라우드 네이티브 환경(예시: 쿠버네티스)에서는 CNAPP 시스템 등을 통해 컨테이너와 워크로드의 런타임 행위를 분석하고, 정의된 정책을 위반하는 이상 행위(예시: 허용되지 않은 프로세스 실행, 악성 C&C 서버 통신 시도)를 실시간으로 탐지하고 자동으로 차단한다.

✓ **모든 소프트웨어 개발 및 통합 프로세스가 자동화되어 있는가?**

- 소프트웨어 개발에 대한 요구사항 정의부터 코드 통합, 보안 테스트, 배포에 이르는 SDLC 전 과정이 완전 자동화된 DevSecOps 체계로 운영된다. 실무 환경에서는 IaC(Infrastructure as Code), GitOps 워크플로우와 통합되어, 개발자가 정책이나 코드를 커밋(Commit)하는 순간부터 SAST/DAST/SCA/IAS T 등의 모든 보안 테스트와 정책 준수 검증이 자동으로 실행된다. 모든 검증을 통과한 경우에만 배포가 자동으로 승인 및 실행되며, 이 모든 개발 및 통합 프로세스는 관리자 개입이 최소화된 자율적인 방식으로 운영된다.

항목	5.5.2 소프트웨어 위험 관리	
설명	소프트웨어 개발 및 운영 과정에서 발생할 수 있는 보안 위험을 식별, 평가, 완화하는 프로세스이다.	
성숙단계	기존	최소한의 위험 요소가 식별되고 문서화하였는가?
		소프트웨어 위험 관리 계획이 수립되어 있는가?
	초기	위험 평가 프로세스를 도입하여 소프트웨어의 위험 수준을 평가하는가?
	향상	소프트웨어 공급망에 대한 보안 강화를 통하여 전주기적 자동화 위험 관리가 이루어지는가?
	최적화	AI 기반 예측 분석을 도입하여 잠재적 보안 위험을 식별할 수 있는가?
		맞춤형 공격에 대응 가능한가?

세부 설명

■ **기존**

✓ **최소한의 위험 요소가 식별되고 문서화 하였는가?**

- 기본적인 SDLC(소프트웨어 개발 생명주기) 기준으로 위험 관리가 이루어지나, 체계적이지 않은 상태이다. 실무 환경에서는 개발 초기 또는 운영 중 발견된 취약점이나 위험 요소를 개발자가 자체적으로 식별하고 비정형적으로 문서화한다. 위험 식별 기준이 조직 전체적으로 일관되지 않고, 기본적인 소프트웨어 개발 보안 가이드에 따라 개발자가 수동으로 조치하고 관리하는 수준에 머무른다.

✓ **소프트웨어 위험 관리 계획이 수립되어 있는가?**

- 발생 가능한 보안 사고(예시: 취약점 발견, 악성코드 감염)에 대비한 기본적인 대응 절차 및 책임 분장(R&R)이 문서화되어 있다. 하지만 이 소프트웨어 위험 관리 계획이 SDLC 전반에 걸쳐 체계적으로 적용되지 않으며, 실질적인 훈련이나 정기적인 검토는 제한적으로 수행된다.

■ **초기**

✓ **위험 평가 프로세스를 도입하여 소프트웨어의 위험 수준을 평가하는가?**

- 위험 평가 프로세스를 도입하여 소프트웨어의 위험 수준을 정량적으로 평가하기 시작한다. 실무 환경에서는 SDLC의 '요구사항 분석' 또는 '설계' 단계에서부터 식별된 위험 요소를 평가한다. 이 단계에서는 SAST/SCA 검사 결과로 나온 취약점에 대해 CVSS(공통 취약점 평가 시스템) 점수나 SVSS(이해관계자별 취약점 평가 시스템) 등을 활용하여 등급을 분류하고, 해당 소프트웨어의 자산 가치(중요도)나 비즈니스 영향도 분석을 통해 리스크를 정량화한다. 이 평가 결과를 바탕으로(예시: 'High' 등급 취약점 우선 조치), 어떤 취약점부터 조치할지에 대한 우선순위 산정 프로세스를 마련하여 운영한다.

■ **향상**

✓ **소프트웨어 공급망에 대한 보안 강화를 통하여 전 주기적 자동화 위험 관리가 이루어지는가?**

- 초기' 단계의 위험 평가를 확장하여, 소프트웨어 공급망 전체로 위험 관리 범위를 확대한다. 실무 환경에서는 SDLC 전반에 걸쳐, 개발 중인 코드뿐만 아니라 사용되는 모든 오픈소스 및 서드파티

구성요소의 공급망 위험까지 포함하여 자동으로 분석을 수행한다. CI/CD 파이프라인에 SCA 도구가 통합되어, 빌드 시마다 SBOM을 자동으로 생성하고, 알려진 취약점(CVE)이 포함된 라이브러리가 있는지 자동으로 스캐닝한다. 탐지된 취약점은 CVSS 점수, 자산 중요도, 외부 위협 인텔리전스(CTI) 정보 등을 종합하여 위험 등급을 자동으로 평가하고, 이에 따른 조치(예시: 'High' 등급 이상일 경우 빌드 차단, 개발자에게 즉시 알림)를 수행하는 등 전 주기적인 자동화 위험 관리가 이루어진다.

■ **최적화**

✓ **AI 기반 예측 분석을 도입하여 잠재적 보안 위험을 식별할 수 있는가?**

- ML/AI 기반의 예측 분석을 도입하여 잠재적 보안 위험을 사전에 식별한다. 실무 환경에서는 DevSecOps 파이프라인의 CI/CD 로그, 과거 취약점 데이터, 개발자의 코드 변경 이력(Commit/PR 패턴), 런타임 환경의 이상 동작 패턴(IAST, RASP) 등 방대한 데이터를 AI 엔진이 학습한다. 이를 통해, 개별 취약점이 아닌 '공격자가 악용할 가능성이 높은 코드'나 '향후 장애를 유발할 수 있는 복잡한 의존성' 등 잠재적인 위험 요소를 사전에 식별하고 개발자에게 경고하여 선제적인 대응을 수행한다.

✓ **맞춤형 공격에 대응 가능한가?**

- 조직의 소프트웨어 개발 환경(SDLC)에 특화된 위협 모델(Threat Model)과 자동 방어 체계를 구축한다. 실무 환경에서는 단순히 취약점을 찾는 것을 넘어, 조직을 대상으로 하는 특정 공격자 전술(TTPs)에 기반한 공격 시뮬레이션(BAS, Breach and Attack Simulation)을 CI/CD 파이프라인과 운영 환경(Runtime)에 대해 정기적/자동으로 수행한다. 이를 통해 발견된 공격 경로(Attack Path)나 취약점을 즉시 식별하고, SIEM/SOAR 시스템과 연동하여 관련 보안 정책(예시: CNAPP/WAAP 룰셋 자동 업데이트, RASP 방어 정책 즉시 적용)을 자율적으로 조정하는 등 맞춤형 공격에 대한 자동화된 대응을 수행한다.

6. 데이터

6.1 데이터 목록 관리

항목	6.1.1 데이터 카탈로그 위험 정렬	
설명	조직의 모든 데이터를 분류하고, 데이터가 식별 및 목록화되고 데이터 환경에 대한 모든 변경 사항이 자동으로 감지되어 카탈로그 내에 포함되는지 확인하는 것을 의미한다. 각 데이터 항목에 대한 위험 수준을 평가하여 이를 체계적으로 관리하는 과정이다.	
성숙단계	기존	데이터 자산의 초기 카탈로그가 작성되어 있는가?
		데이터를 파악하고, 유형 분류를 수동으로 하는가?
		데이터에 대한 기본적인 위험 평가를 문서화하였는가?
	초기	자동화된 데이터 카탈로그 도구가 도입되어 있는가?
		데이터 자산을 일부 자동으로 수집하고 분류하는가?
		데이터 위험 수준 평가를 위하여 기본적인 기준과 지침이 마련되어 있는가?
	향상	데이터의 민감도와 위험 수준을 평가하기 위한 분석 도구가 있는가?
		데이터를 자동화하여 파악하고, 위험한 데이터에 대한 보호 정책이 적용되어 있는가?
		데이터 사용 패턴 분석이 가능한가?
	최적화	AI 기반 데이터 위험 요소를 실시간으로 분석하는가?
		데이터 카탈로그와 다른 보안 시스템이 통합되어 관리되는가?

세부 설명

■ **기존**

✓ **데이터 자산의 초기 카탈로그가 작성되어 있는가?**

- 조직 내 보유한 데이터의 위치(예시: 파일 서버, DB, PC), 포맷, 보유 시스템 등을 식별하여, 스프레드시트나 자산관리 문서 등을 활용해 수동으로 목록(카탈로그)을 작성하여 관리하기 시작한다.

✓ **데이터를 파악하고, 유형 분류를 수동으로 하는가?**

- 데이터를 파악하고, 유형 분류를 수동으로 수행한다. 실무 환경에서는 조직의 일반 보안 정책이나 컴플라이언스(예시: 개인정보보호법, 정보통신망법, 신용정보법 등) 기준에 따라, 데이터를 '일반 데이터'와 '개인정보가 포함된 데이터' 수준으로 단순 분류하는 단계이다. 이 분류를 기준으로 기본적인 보안 정책(예시: 개인정보 포함 DB는 암호화 적용)이 적용되기 시작한다.

✓ **데이터에 대한 기본적인 위험 평가를 문서화 하였는가?**

- 분류된 데이터의 민감도와 자산 중요도, 보안 요구사항 등을 중심으로 정성적인 위험 평가를 수행하고 그 결과를 문서화한다. 실무 환경에서는 이 위험 등급이 '일반' 또는 '민감(개인정보)' 등 내부 관리 기준에 따라 단순 정의되며, 아직 체계적인 평가 프레임워크가 적용되지는 않은 상태이다.

■ **초기**

✓ **자동화된 데이터 카탈로그 도구가 도입되어 있는가?**

- 자동화된 데이터 카탈로그 도구(예시: DSPM, eDLP, eDRM 등)를 도입하여, 다양한 데이터가 생성될 때나 저장소(예시: 온프레미스 DB, 클라우드 스토리지, SaaS)의 메타데이터를 자동으로 수집하기 시작한다. 이 도구를 통해 수동 관리(스프레드시트)에서 벗어나, 조직의 데이터 자산을 식별하고 사전 정의된 규칙에 따라 카탈로그화하는 기반을 마련한다.

✓ **데이터 자산을 일부 자동으로 수집하고 분류하는가?**

- 데이터 카탈로그 도구나 eDLP, eDRM, DB암호화 등 연계 솔루션을 통해 특정 저장소(예시: DB, S3, 파일서버)에 있는 데이터의 포맷, 이름, 구조 등을 기반으로 일부 자동 분류를 수행한다. 이 단계에서는 '일반 데이터'와 '개인정보 포함 데이터' 수준을 넘어, 조직의 업종과 특성을 고려한 데이터 등급(예시: '대외 유통 가능', '조직 내부 전용', '직책자 전용')을 정의하기 시작한다. 이 분류 기준에 따라 일부 민감 정보에 대한 데이터 태깅을 수행한다.

✓ **데이터 위험 수준 평가를 위하여 기본적인 기준과 지침이 마련되어 있는가?**

- 수동 및 일부 자동화된 분류 결과를 바탕으로, 데이터의 민감도, 접근권한, 저장 위치, 사용 주체 등을 고려한 위험 평가 기준과 지침을 수립하여 평가 표준화를 시작한다. 실무 환경에서는 정의된 데이터 등급(예시: '조직 내부 전용', '직책자 전용')에 따라 차등화된 보안 정책을 적용하기 위한 기준을 마련한다.(예시: '직책자 전용' 등급의 데이터는 eDRM을 통한 암호화 및 열람 권한 제어를 적용하고, '조직 내부 전용' 데이터의 외부 반출 시에는 별도 결재 프로세스를 적용)

■ **향상**

✓ **데이터의 민감도와 위험 수준을 평가하기 위한 분석 도구가 있는가?**

- 데이터 보안 형상 관리(DSPM) 시스템이나 이와 유사한 전문 분석 도구를 도입한다. 실무 환경에서는 이러한 도구가 ML/NLP(머신러닝/자연어 처리) 기반의 분석을 통해 데이터 내용 자체를 스캔하고, PII(개인식별정보), PHI(개인건강정보), 금융정보 등 정형/비정형 데이터에 포함된 민감 정보를 자동으로 식별하고 분류한다. 이 결과를 바탕으로 데이터의 민감도와 비즈니스 영향도를 조합하여 정량화된 데이터별 위험 스코어링을 수행한다.

✓ **데이터를 자동화하여 파악하고, 위험한 데이터에 대한 보호 정책이 적용되어 있는가?**

- 자동화된 데이터 파악(Discovery) 및 분류 결과를 바탕으로, 위험한 데이터에 대한 보호 정책이 자동으로 적용된다. 실무 환경에서는 DSPM, eDLP, eDRM 등의 시스템이 연동되어, 이전 단계에서 정의한 데이터 등급(예시: '직책자 전용')이나 '위험 점수'가 높은 항목(예시: 개인정보 100건 이상이 포함된 문서)에 대해 eDRM 암호화, 데이터 접근제어 강화, 외부 이동 방지(DLP 차단) 등의 보호 정책이 자동으로 적용된다.

✓ **데이터 사용 패턴 분석이 가능한가?**

- 데이터 자체의 분류를 넘어, '누가' '언제' '어떻게' 해당 데이터에 접근하고 사용하는지에 대한 패턴 분석이 가능해진다. 실무 환경에서는 DSPM, UEBA, SIEM/SOAR 등의 시스템이 연동되어, 데이터 접근 로그(예시: DB 접근 로그, 파일 서버 로그)를 수집한다. 이를 통해 평소와 다른 시간대의 접근, 과도한

양의 데이터 다운로드 시도, 휴면 계정의 민감 데이터 접근 등 이상 행위를 탐지하고, 이 분석 결과를 실시간 위험 정렬에 반영하여 경고를 발생시킨다.

■ **최적화**

✓ **AI 기반 데이터 위험 요소를 실시간으로 분석하는가?**

- ML/AI 기반 엔진이 정적 위험 평가를 넘어, 실시간으로 조직 내 모든 데이터 저장소(예시: 온프레미스 DB, 클라우드 스토리지, SaaS)를 지속적으로 모니터링한다. 실무 환경에서는 DSPM 시스템 등이 AI 엔진을 활용하여, 새로운 데이터 항목의 생성, 민감도(예시: PII, 기밀 정보) 자동 분류, 데이터 접근 패턴, 사용자 간 공유/연관성 등을 실시간으로 분석한다. 이 분석 결과는 데이터의 동적인 위험 점수로 산출되며, 데이터 카탈로그에 자동으로 반영되어 항상 최신 위험 상태를 유지한다.

✓ **데이터 카탈로그와 다른 보안 시스템이 통합되어 관리되는가?**

- 데이터 카탈로그가 중앙 정책 엔진(PDP)(예시: ICAM) 및 SIEM/SOAR, eDLP, eDRM, ZTNA, CNAPP, CASB 등 다른 보안 시스템과 유기적으로 통합되어, 종합적인 데이터 중심 보안 관리가 이루어진다. 실무 환경에서는 AI가 실시간으로 분석한 데이터 위험 점수(예시: '고위험 기밀 데이터')가 정책 엔진(ICAM)에 즉시 연동된다. 정책 엔진은 이 정보를 바탕으로 '해당 데이터는 다운로드 불가'와 같은 동적 접근 정책을 결정하며, 이 정책은 eDLP, ZTNA, CASB 등 정책시행지점(PEP)에 자동으로 적용되어 데이터 유출 방지 및 정책 적용, 위협 탐지가 자동화된 방식으로 연동된다.

항목	6.1.2 기업 데이터 거버넌스	
설명	조직 내 모든 데이터의 사용, 보호, 관리에 대한 규칙과 절차를 정의하고, 이를 준수하는 과정을 의미한다.	
성숙단계	기존	데이터 거버넌스 정책 수립 및 데이터 관리에 대한 기본적인 지침이 마련되어 있는가?
		데이터 소유자와 관리자를 지정하였는가?
		데이터 거버넌스 프레임워크가 도입되어 있는가?
	초기	데이터 정책 준수를 위하여 정기적인 감사와 검토가 수행되는가?
	향상	데이터 거버넌스 도구를 이용하여 데이터 관리 프로세스를 자동화하였는가?
		데이터 정책 준수에 대한 실시간 모니터링이 가능한가?
	최적화	데이터 거버넌스를 조직의 모든 시스템과 통합하여 일관된 데이터 관리가 가능한가?

세부 설명

■ **기존**

✓ **데이터 거버넌스 정책 수립 및 데이터 관리에 대한 기본적인 지침이 마련되어 있는가?**

- 데이터의 생성, 수집, 처리, 저장, 폐기 등 전체 생명주기에 대해 조직 내에서 준수해야 할 기본적인 규칙과 절차를 문서화한다. 실무 환경에서는 주로 개인정보보호법 등 관련 규제(컴플라이언스) 준수를 위한 최소한의 기반을 마련하는 수준이며, 보안 정책이나 지침서 내에 데이터 관리 원칙이 포함되어 있다.

✓ **데이터 소유자와 관리자를 지정하였는가?**

- 각 데이터 자산(예시: 인사DB, 재무데이터)에 대해, 정책적 책임을 지는 '소유자(Data Owner)'(예시: 인사팀장)와 실무적인 관리를 담당하는 '관리자(Data Steward)'(예시: IT팀 DB 관리자)를 명시하여 책임 구역(R&R)을 정의한다. 이 단계에서는 이러한 지정이 공식적으로 문서화되어 있으나, 실제 권한 통제 시스템과 자동화되어 연계되지는 않는다.

✓ **데이터 거버넌스 프레임워크가 도입되어 있는가?**

- 데이터 품질, 보안, 접근제어 등 데이터 통제 영역을 데이터 목록 관리 및 분류에서 정의한 기본적인 거버넌스 체계(프레임워크) 초안을 수립하고 문서화한다. 이 프레임워크는 조직의 데이터 관리 방향성을 제시하지만, 아직 전사적으로 강제되거나 자동화된 도구를 통해 구현되지는 않은 상태이다. 이 단계에서는 데이터 거버넌스가 실무자 수준에서 논의되거나, 공식적인 전사 기구(예시: 데이터 위원회)가 아닌 IT/보안 부서 내부의 협의체 수준에서 다루어진다.

■ **초기**

✓ **데이터 정책 준수를 위하여 정기적인 감사와 검토가 수행되는가?**

- '기존' 단계에서 문서화된 데이터 거버넌스 프레임워크를 체계화하고, 조직의 업종과 특성을 고려하여 데이터를 다양한 형태의 등급(예시: '대외 유통 가능', '조직 내부 전용', '직책자 전용' 등)으로 모두 정의한다. 이러한 데이터 등급과 정책은 실무 부서(예시: 현업, IT, 보안) 담당자들이 참여하는 공식 협의체를 통해 결정된다. 이 정의된 데이터 등급에 맞춰, 민감도, 암호화, 보관 주기, 반출 및 결재 프로세스(예시: '직책자 전용' 등급은 eDRM 암호화 적용, '조직 내부 전용' 등급은 eDLP 외부 반출 차단) 등 구체적인 보호 조치를 정책화한다. 실무 환경에서는 이 정책이 실제 시스템에 일관되게 적용되고 있는지 확인하기 위해, 정기적으로(예시: 반기별, 연간) 데이터 접근 기록, 품질, 보안 위반 여부 등을 점검하는 감사 및 검토를 수행한다.

■ **향상**

✓ **데이터 거버넌스 도구를 이용하여 데이터 관리 프로세스를 자동화하였는가?**

- 데이터 거버넌스 도구(예시: DSPM, eDLP, eDRM, DB 암호화 등)를 이용하여 데이터 관리 프로세스를 자동화한다. 이전 단계 단계에서 수립된 데이터 분류 체계, 데이터 소유권 지정, 정책 매핑 등 반복되는 관리 작업을 자동화하여 정책 누락이나 인적 오류를 방지한다. 실무 환경에서는 변화하는 법규(예시: 개인정보보호법 개정)나 비즈니스 요구사항에 따라 데이터 거버넌스 도구를 통해 정책을 자동으로 수정하고, 이를 적용 대상 전체(예시: 전사 DB, 클라우드 스토리지)에 반영하는 것을 의미한다.

✓ **데이터 정책 준수에 대한 실시간 모니터링이 가능한가?**

- 데이터 거버넌스 도구와 UEBA, SIEM/SOAR 등의 시스템을 연동하여, 데이터 정책 준수 여부에 대한 실시간 모니터링을 수행한다. 실무 환경에서는 민감 데이터 접근, 비정상 활동, 정의된 정책(예시: eDLP 반출 정책) 위반 등을 실시간으로 감지하고 알림을 전송하거나 접근을 차단하며, 이 분석 결과를 거버넌스 정책에 지속적으로 피드백한다.

■ **최적화**

✓ **데이터 거버넌스를 조직의 모든 시스템과 통합하여 일관된 데이터 관리가 가능한가?**

- 데이터 거버넌스가 실무자와 경영진이 포함된 전사적 기구(예시: 데이터 위원회, 디지털 위원회)를 통해 조직 차원에서 다루어진다. 실무 환경에서는 이 전사 기구를 통해 데이터 거버넌스 정책이 결정되며, 이 정책은 ML/AI 기반의 거버넌스 관리 시스템(예시: DSPM, eDLP, eDRM, SIEM/SOAR 등)을 통해 전사 모든 시스템(예시: 온프레미스, 클라우드, SaaS)에 실시간으로 반영되고 통합된다. ML/AI 엔진이 데이터의 생성, 변경, 폐기 등 전체 생명주기를 지속적으로 모니터링하며, 정책 준수 여부를 실시간으로 평가하고 자동 최적화한다. 이를 통해 수립된 일관된 데이터 관리 정책은 ICAM, ZTNA, eDLP 등 다른 제로트러스트 보안 시스템과 유기적으로 통합되어, 기술적인 통제와 관리적인 거버넌스가 하나의 체계로 운영된다.

6.2 접근 결정방법

항목	6.2.1 데이터 접근제어	
설명	데이터를 보호하기 위해 데이터에 접근할 수 있는 권한을 부여하고, 이를 엄격하게 관리하는 과정이다. 데이터 및 사용자/NPE/장치 속성을 기반으로 데이터에 대한 적절한 접근 및 사용을 보장하여야 한다.	
성숙단계	기존	데이터 접근 정책이 수립되어 있는가?
		데이터 접근권한이 수동으로 부여되는가?
	초기	중앙 집중식 접근제어 시스템이 도입되어 있는가?
		최소한의 권한 요소를 확인하여 데이터 접근 여부를 결정하는가?
	향상	ABAC을 통하여 컨텍스트 기반으로 접근권한 관리가 구현되어 있는가?
	최적화	데이터 접근제어를 최소화하고 AI를 이용하여 데이터 접근에 대한 실시간 권한 조정이 가능한가?

세부 설명

■ **기존**

✓ **데이터 접근 정책이 수립되어 있는가?**

- 조직의 중요 데이터(예시: 개인정보 DB, DB서버)에 접근할 수 있는 사용자와 권한을 정의한 정책이 존재하며, 주로 엑셀이나 내부 지침 등 문서 형태로 수립되어 있다. 실무 환경에서는 이 정책이 별도 DB접근제어 시스템이나 PAM 시스템 내에 정적인 규칙(Rule)으로 수동 설정되어 적용된다.

✓ **데이터 접근권한이 수동으로 부여되는가?**

- 사용자의 직무나 개별 요청(예시: 그룹웨어 결재, 메일 요청)에 따라, 보안 관리자(또는 DB 관리자)가 데이터 접근제어 시스템(예시: DB접근제어, PAM)에 접속하여 직접 권한을 부여하거나 회수한다. 이 단계에서는 IDP 역할을 하는 Directory, IAM, PAM 등 중앙 식별자 관리 시스템과 부분적으로 연동되거나, 연동되지 않아 계정 정보나 권한이 실시간으로 동기화되지 않으며 인적 실수로 인한 최소 권한 부여에는 한계점이 존재한다.

■ **초기**

✓ **중앙 집중식 접근제어 시스템이 도입되어 있는가?**

- 개별/수동 관리를 벗어나, 데이터 접근제어를 위한 중앙 집중식 접근제어 시스템(예시: DB 접근제어 시스템, PAM)이 전사적으로 확대된다. 실무 환경에서는 모든 DB 서버나 파일 서버에 대한 데이터 접근 경로가 이 중앙 플랫폼을 통해서만 접근 가능하도록 통합되며, 역할(Role) 기반 또는 부서 기반으로 권한 설정을 관리하기 시작한다.

✓ **최소한의 권한 요소를 확인하여 데이터 접근 여부를 결정하는가?**

- 포괄적인 서버 접근(예시: 서버 접근 후 서버 내 DB 접근)과 달리, RBAC(역할 기반 접근제어)를 기반으로 최소 권한 원칙을 적용하여 업무상 필요한 범위의 데이터(예시: 특정 테이블, 특정 쿼리)에 대한 접근 여부를 결정한다. 이 단계에서는 아직 중앙 IDP(예시: IAM, ICAM)와 실시간으로 연동되지는 않더라도, 데이터 접근제어 시스템(예시: DB 접근제어, PAM) 내에서 정의된 역할(Role)과 정책을 기반으로 최소한의 권한을 부여하고 접근을 통제한다.

■ **향상**

✓ **ABAC을 통하여 컨텍스트 기반으로 접근권한 관리가 구현되어 있는가?**

- ABAC(속성 기반 접근제어)을 도입하여, 정적 역할(Role)뿐만 아니라 다양한 컨텍스트(속성)를 기반으로 접근권한 관리를 구현한다. 실무 환경에서는 데이터 접근제어 시스템(예시: DB 접근제어, PAM)이 중앙 IDP(예시: IAM, ICAM)와 연동되어, 사용자의 속성(예시: 부서, 직책)을 실시간으로 가져온다. 또한, 사용자 위치, 기기 보안 상태, 업무 맥락(예시: 접속 시간) 등 다양한 요소를 정책 엔진이 평가하여, 세분화된 정책 적용이 가능하다. 나아가, eDLP, SIEM/SOAR 시스템과 연동하여, '민감 데이터 유출 시도'와 같은 보안 이벤트가 탐지되면 이에 따라 데이터 접근권한을 동적으로 조정(예시: 해당 계정의 DB 접근 차단)하고 이상 탐지 시 접근을 차단한다.

■ **최적화**

✓ **데이터 접근제어를 최소화하고 AI를 이용하여 데이터 접근에 대한 실시간 권한 조정이 가능한가?**

- 데이터 접근제어를 최소화하고 ML/AI을 활용하여 데이터 접근에 대한 실시간 권한 조정이 자율적으로 이루어진다. 실무 환경에서는 데이터 카탈로그 정책에 맞춰서 식별된 데이터 등급분류 정보와 SIEM/SOAR를 통해 수집/분석된 사용자 행동 패턴(UEBA), 접근 로그, 데이터 민감도 정보가 중앙 정책 엔진(PDP)인 ICAM에 실시간으로 전달된다. ICAM, SIEM/SOAR 시스템 등은 해당 정보들을 ML/AI로 분석하여 동적인 위험 점수를 스코어링하며, 이 점수에 맞게 데이터 접근권한(예시: JIT/JE A 기반의 최소 권한)을 PDP에서 결정한다. 이 결정된 정책은 실제 데이터 접근을 수행하는 정책시행지점(PEP)(예시: PAM, eDLP, eDRM 등)에 전달되어, 권한을 실시간으로 조정하거나 이상 징후 탐지 시 자동으로 접근을 차단한다. 또한 업무 변동, 사용자 역할 변경, 새로운 데이터 생성 시에도 이 접근제어 정책이 자동으로 갱신되며, 전사적 보안 정책과 연계된다.

6.3 데이터 암호화

항목	6.3.1 데이터 암호화 및 권한 관리	
설명	데이터의 무결성과 기밀성을 보호하기 위해 데이터를 암호화하고, 접근권한을 관리하는 과정이다. 저장 및 전송 중인 데이터를 암호화하기 위한 전략을 수립하고 구현하여야 한다.	
성숙단계	기존	데이터를 수동으로 암호화하는가?
		암호화 정책이 수립되어 있는가?
		데이터를 보호하기 위한 초기 권한 관리 체계가 수립되어 있는가?
	초기	자동화된 암호화 도구를 통하여 중요한 데이터를 자동으로 암호화하는가?
		중앙 집중식 데이터 권한 관리 시스템이 도입되어 있는가?
	향상	고급 암호화 기술을 도입하고, 권한 관리 시스템과 통합하여 관리하고 있는가?
		RBAC과 ABAC을 결합하여 보다 정밀한 권한 관리가 이루어지는가?
	최적화	AI 기반 암호화 및 권한 관리를 통하여 데이터 보호 최적화 및 실시간 권한 조정이 가능한가?

세부 설명

■ **기존**

✓ **데이터를 수동으로 암호화하는가?**

- 조직의 체계적인 암호화 전략이 부재하여, 특정 중요 파일에 대해서만 수동으로 암호화를 수행한다. 실무 환경에서는 문서 자체 암호(예시: MS 오피스 암호 설정, 압축파일 암호)를 적용하는 수준에 머무르며, DB 암호화나 eDRM 같은 자동화된 시스템이 도입되지 않았거나, 도입되었더라도 전사적으로 적용되지 않고 특정 영역에 한정된 상태이다.

✓ **암호화 정책이 수립되어 있는가?**

- 암호화 대상 데이터(예시: 개인정보), 사용 알고리즘, 키 관리 방식 등이 내부 보안 지침이나 정책서에 문서화되어 있다. 하지만, 이 정책이 실제 시스템에 일관되게 적용(강제)되지 않으며, 암호화 키 관리가 중앙화된 시스템(예시: KMS 시스템) 없이 담당자가 수동으로 관리하는 등 체계적인 관리가 부재하다.

✓ **데이터를 보호하기 위한 초기 권한 관리 체계가 수립되어 있는가?**

- 암호화된 데이터를 보호하기 위한 초기 권한 관리 체계가 수립되어 있다. 실무 환경에서는 eDRM 시스템 등이 도입되어 정형 데이터와 비정형 데이터에 대한 접근권한(예시: 열람, 편집, 인쇄, 캡처 방지)을 정의할 수 있다. 하지만 이 권한 분류가 데이터 카탈로그나 사용자 인벤토리와 연동되지 않고, 업무 담당자(소유자)가 수동으로 권한을 적용하는 등 표준화된 중앙 접근제어 시스템(예시: PAM)과는 통합되지 않은 상태이다.

■ **초기**

✓ **자동화된 암호화 도구를 통하여 중요한 데이터를 자동으로 암호화하는가?**

- 수동 암호화에서 벗어나, 자동화된 암호화 도구를 도입하여 중요한 데이터를 보호하기 시작한다. 모든 데이터를 암호화할 경우 성능 저하(예시: 데이터 조회 및 전송 지연)가 발생할 수 있으므로, 실무 환경에서는 데이터 거버넌스 및 데이터 분류 체계에 따라 정의된 중요 데이터(예시: 개인정보, 기밀 문서)에 한해 암호화가 적용된다. 이는 콘텐츠 중앙화(ECM) 시스템, DB암호화 솔루션(정형 데이터), eDRM(비정형 데이터) 등을 통해 구현되며, 데이터 저장 시 파일·디렉토리 단위 또는 데이터베이스 필드 단위까지 암호화를 수행한다.

✓ **중앙 집중식 데이터 권한 관리 시스템이 도입되어 있는가?**

- 데이터 암호화와 연계되어, eDRM이나 DB 접근제어, PAM 등 시스템 내에서 데이터 접근권한 관리가 중앙 집중화되기 시작한다. 실무 환경에서는 IDP(IAM 등) 시스템과 연동하여, 사용자의 역할(Role)이나 그룹 정보를 기반으로 암호화된 데이터(문서, DB 테이블)에 대한 접근권한(예시: 열람, 편집, 인쇄)을 중앙에서 승인/회수하는 체계를 구축하기 시작한다.

■ **향상**

✓ **고급 암호화 기술을 도입하고, 권한 관리 시스템과 통합하여 관리하고 있는가?**

- AES-256, TLS 1.3 등 강력한 암호화 기술을 기반으로 저장 데이터(Data-at-Rest)와 전송 중인 데이터(Data-in-Transit)를 보호한다. 실무 환경에서는 DB 암호화, eDRM 시스템 등이 전사적으로 적용되며, 암호화 시 키의 생성, 배포, 회전, 폐기 등 전체 생명주기를 관리하기 위한 중앙 집중식 키 관리 시스템(KMS, ICAM 등)이 도입되어 운영된다.

✓ **RBAC과 ABAC을 결합하여 보다 정밀한 권한 관리가 이루어지는가?**

- 암호화된 데이터에 대한 권한 관리가 단순 역할 기반을 넘어, 정적인 RBAC(역할 기반)과 동적인 ABAC(속성 기반)을 결합하여 정밀하게 이루어진다. 실무 환경에서는 eDRM, eDLP, PAM 시스템 등과 같은 권한 관리 시스템이 중앙 정책 엔진(PDP)(예시: ICAM)과 연동되어, 사용자의 역할(예시: '인사팀') 뿐만 아니라 컨텍스트(예시: '사무실 내 접속', '보안 등록 기기')까지 결합하여 데이터 접근 조건을 상세화하고 보다 정밀한 제어를 수행한다.

■ **최적화**

✓ **AI 기반 암호화 및 권한 관리를 통하여 데이터 보호 최적화 및 실시간 권한 조정이 가능한가?**

- ML/AI 기반의 UEBA기능이 데이터 암호화 및 권한 관리 체계에 통합된다. 실무 환경에서는 SIEM/SOAR, DSPM 등에서 수집된 사용자 행동 패턴, 데이터 사용 이력, 기기 상태 등을 AI 엔진이 실시간으로 분석하여 동적인 위험 점수를 산출한다. 이 점수는 중앙 정책 엔진(PDP)(예시: ICAM)으로 전달되며, 정책 엔진은 위험도에 따라 암호화된 데이터(문서 등)에 대한 접근권한(예시: 열람, 편집, 인쇄)을 자동으로 조정(예: '편집' 권한을 '읽기 전용'으로 하향)하거나 차단하는 등의 조치를 정책시행지점(PEP)에 해당하는 eDRM. DB 암호화, 키 관리 시스템 등을 통해 실시간으로 수행한다.

✓ **데이터에 대하여 실시간 권한에 따른 마스킹이 가능한가?**

- 데이터에 대한 실시간 권한에 따른 동적 마스킹이 구현된다. 실무 환경에서는 사용자의 권한 수준(예시: 일반 사용자 vs. 인사팀 관리자) 및 컨텍스트(예시: 사내망 vs. 외부망)에 따라, 동일한 데이터(예시: 고객 테이블)에 접근하더라도 개인정보나 민감정보(예시: 건강정보, 생체인식 정보 등)가 실시간으로 마스킹('***')되거나 일부만 가공되어 출력된다. 이는 DB 접근제어 솔루션, PAM 또는 애플리케이션 레벨에서 정책 엔진(PDP)의 결정을 받아 정책시행지점(PEP)에서 수행되며, 민감 데이터 노출을 최소화하면서 업무 연속성을 보장한다.

6.4 데이터 분류

항목	6.4.1 데이터 라벨링 및 태그 지정	
설명	데이터를 식별하고 분류하기 위해 메타데이터를 추가하는 과정이다. 데이터 소유자는 레이블 지정/태깅 정책에 대한 관리 지침을 준수하여 데이터 레이블을 지정하고 태그를 지정한다. 단계가 발전함에 따라 자동화되며, 확장 요구사항을 충족하고 더 나은 정확성을 제공하여야 한다. 이를 통해 데이터의 보안 수준을 강화할 수 있다.	
성숙단계	기존	라벨링 및 태그 지정 지침을 수립하였는가?
		일관된 데이터 분류 체계가 마련되어 있는가?
	초기	데이터에 기본적인 라벨과 태그를 수동으로 지정하여 식별·분류하는가?
		민감한 데이터에 특수 라벨을 적용할 수 있는가?
		민감한 데이터에 보안 정책이 차등적으로 적용되는가?
	향상	자동화된 라벨링 및 태그 지정 도구를 도입하여 자산을 자동으로 분류·식별 가능한가?
		타 보안 시스템과 연계하여 데이터 보호가 가능한가?
	최적화	고급 메타데이터 관리 도구를 통하여 데이터 라벨링과 태그 지정 프로세스를 적용하는가?
		AI를 활용하여 변화하는 데이터 환경에 따른 분류가 자동 조정되는가?

세부 설명

■ **기존**

✓ **라벨링 및 태그 지정 지침을 수립하였는가?**

- 조직 내 데이터의 보안 등급, 민감도, 중요도(예시: '대외비', '기밀', '공개') 등에 따른 라벨 및 태그 지정 기준을 문서화한다. 이 단계에서는 데이터 거버넌스에서 정의한 분류 체계를 실제 데이터에 어떻게 부착할 것인지에 대한 초기 지침을 의미하며, 아직 자동화된 도구 없이 관리자가 수동으로 시스템이나 데이터에 보안 등급(라벨)을 적용하기 시작한다.

✓ **일관된 데이터 분류 체계가 마련되어 있는가?**

- 데이터의 민감도(예시: '개인정보 포함', '일반') 및 부서/업무 기반의 기본적인 데이터 분류 체계는 마련되어 있다. 하지만 이 분류 체계(라벨링)가 전사적으로 일관되게 적용되지 않으며(예시: A 부서는 '대외비', B 부서는 '기밀' 등 용어 혼용), 자동화된 시스템이 부재하여 실제 데이터와 정책(라벨) 간의 일관성이 보장되지 않는 상태이다.

■ **초기**

✓ **데이터에 기본적인 라벨과 태그를 수동으로 지정하여 식별·분류하는가?**

- 데이터 거버넌스에서 정의한 데이터 분류 체계(예시: '대외 유통 가능', '조직 내부 전용', '직책자 전용' 등)를 바탕으로, 사용자가 파일 저장 또는 문서 작성 시 수동으로 데이터에 라벨과 태그를 지정하여 식별·분류하기 시작한다.

✓ **민감한 데이터에 특수 라벨을 적용할 수 있는가?**

- 정의된 데이터 분류 체계(예시: '대외 유통 가능', '조직 내부 전용', '직책자 전용' 등)의 일반적인 라벨 외에도, 관련 법규(컴플라이언스)나 정책상 민감도가 높은 데이터(예시: PII, PHI, 금융정보)에 대해 '민감' 또는 '개인정보 포함'과 같은 특수 라벨(Tag)을 적용하여 별도로 식별하고 관리한다.

✓ **민감한 데이터에 보안 정책이 차등적으로 적용되는가?**

- 민감' 또는 '개인정보 포함' 라벨이 적용된 데이터에 대해, 다른 데이터와 차등화된 보안 정책이 적용되기 시작한다. 실무 환경에서는 eDLP 시스템과 연동하여, 해당 라벨이 부착된 데이터의 외부 공유를 제한하거나, eDRM 시스템을 통해 기본적인 접근권한(예시: 읽기/인쇄 제한)을 적용하는 등 초기 수준의 정책이 적용된다.

■ **향상**

✓ **자동화된 라벨링 및 태그 지정 도구를 도입하여 자산을 자동으로 분류·식별 가능한가?**

- 자동화된 라벨링 및 태그 지정 도구(예시: DSPM, eDLP, eDRM 등)를 도입하여 자산을 자동으로 분류·식별한다. 실무 환경에서는 eDLP 솔루션이나 DSPM 시스템이 개인정보 포함 여부(예시: 주민번호 패턴), 특정 키워드(예시: '대외비', '기밀') 등 데이터 거버넌스에서 정의된 규칙에 따라 데이터 내용(Content)을 스캔하고, 자동으로 라벨링 및 태그를 지정한다.

✓ **타 보안 시스템과 연계하여 데이터 보호가 가능한가?**

- 자동으로 부착된 라벨(Tag) 값에 따라, 타 보안 시스템과 연계하여 데이터 보호 정책이 자동으로 적용되도록 보안 시스템 간 연동이 이루어진다. 실무 환경에서는 데이터에 '기밀' 라벨이 지정되면, 이 정보가 연동된 eDLP 시스템에서 해당 데이터의 외부 반출을 자동으로 차단하거나, eDRM 시스템이 문서 암호화 및 권한 제어 정책을 자동으로 적용하는 등, 데이터의 분류 등급(라벨)에 따라 보안 시스템이 연동되어 데이터 보호가 수행된다.

■ **최적화**

✓ **고급 메타데이터 관리 도구를 통하여 데이터 라벨링과 태그 지정 프로세스를 적용하는가?**

- 고급 메타데이터 관리 도구(예시: DSPM, eDLP, SIEM/SOAR)를 통하여 데이터 라벨링과 태그 지정 프로세스를 적용한다. 실무 환경에서는 데이터의 내용뿐만 아니라 데이터 소스, 위치, 접근권한, 사용자 속성(예시: ICAM의 사용자 등급) 등 다양한 메타데이터를 자동으로 수집하고, 이를 기반으로 복합적인 라벨링 규칙을 적용한다. 특히, 마이크로 세그멘테이션 시스템과 연동하여, 워크로드나 애플리케이션에 적용된 태그(Tag) 정보를 데이터 분류 및 태깅에 활용하는 등 데이터 단위까지 태깅을 고도화한다.

✓ **AI를 활용하여 변화하는 데이터 환경에 따른 분류가 자동 조정 되는가?**

- ML/AI을 활용하여 변화하는 데이터 환경에 따라 분류가 자동으로 조정된다. 실무 환경에서는 SIEM /SOAR, ICAM(중앙 정책 엔진) 시스템 등 전사 보안 체계에서 데이터 라벨 정보를 실시간으로 공유하고 통합 정책을 수행한다. ML/AI 엔진이 데이터 변경 패턴이나 사용자 접근 패턴을 지속적으로 학습/분석하여, 기존 라벨을 자동으로 수정하거나 태그를 갱신(예시: '일반' 문서를 '기밀'로 자동 상향)하는 등 자율적인 분류 및 정책 조정이 이루어진다.

6.5 데이터 손실 방지

항목	6.5.1 데이터 손실 방지 (DLP)	
설명	민감한 데이터의 유출을 방지하고, 데이터의 무단 접근을 차단하기 위한 기술과 정책이다. 시행 지점을 식별하여 승인된 DLP 도구를 배포하고 태그가 지정된 데이터 속성을 DLP와 통합한다. 처음에 DLP 솔루션은 비즈니스 영향을 제한하기 위해 "모니터링 전용" 모드로 사용하고 나중에 분석 사용은 "방지" 모드로 사용한다. 이후, AI와 통합하여 사용한다.	
성숙단계	기존	DLP 정책을 수립하고 수동으로 평가하는가?
		DLP 도입을 위한 기업 내 범위가 지정되어 있는가?
	초기	DLP 도구를 도입하여 주요 데이터 유출 경로를 모니터링할 수 있는가?
		DLP 정책을 중앙에서 관리하는가?
		DLP 솔루션이 모니터링 모드로 동작하는가?
	향상	DLP 시스템이 전체적으로 도입되어 실시간으로 데이터를 보호하고 유출을 방지하는가?
		DLP 솔루션이 방지 모드로 사용되는가?
	최적화	DLP 시스템에 AI를 적용하여 데이터 유출 위험을 실시간으로 예측하고 차단할 수 있는가?
		변화하는 데이터 환경에 맞춰 자동으로 보안 정책이 최적화되는가?

세부 설명

■ **기존**

✓ **DLP 정책을 수립하고 수동으로 평가하는가?**

- 데이터 손실 방지(DLP)의 개념을 이해하고, 조직 내부 문서(예시: 정보보호 정책/지침)를 통해 민감 정보(예시: 개인정보, 기밀)를 정의하고 기본적인 보호 정책을 수립한다. 이 단계에서는 전용 DLP 시스템이 부재하여, 실제 유출 위험은 방화벽 로그나 파일 서버 접근 로그 등을 수동으로 분석하고 사후에 평가하는 수준에 머무른다.

✓ **DLP 도입을 위한 기업 내 범위가 지정되어 있는가?**

- 전사적인 DLP 도입보다는, 데이터 손실 방지가 필요한 기업 내 범위를 지정(목록화)한다. 실무 환경에서는 이메일, USB/외장하드, 프린터, 웹 업로드, 클라우드 환경 등 주요 데이터 유출 경로(채널)를 식별하고 적용 우선순위를 설정한다. 특히 이 단계에서는 엔드포인트에 설치되는 AV, EPP 등을 활용해 기본적인 DLP 기능에 해당하는 USB나 외장하드로의 데이터 유출을 통제하거나 이메일(예시: 오피스) 자체적인 DLP 기능과 네트워크 방화벽의 DLP 기능 등을 활용하여 기초 수준의 데이터 손실을 방지한다.

■ **초기**

✓ **DLP 도구를 도입하여 주요 데이터 유출 경로를 모니터링할 수 있는가?**

- '기존' 단계에서 식별된 주요 데이터 유출 경로(채널)에 대해 데이터 흐름을 탐지하는 초기 DLP 솔루션이 적용되기 시작한다. 실무 환경에서는 엔드포인트 DLP(eDLP) 시스템을 도입하여 USB, 프린터 등 매체제어를 수행하거나, 네트워크 DLP 시스템을 통해 이메일(SMTP), 웹(HTTP/HTTPS) 등 주요 채널을 통해 전송되는 데이터를 모니터링하는 수준을 의미한다.

✓ **DLP 정책을 중앙에서 관리하는가?**

- 개별 시스템(예시: 방화벽)에서 데이터 손실 방지 기능을 확장하여, DLP 전용 시스템의 중앙 관리 포털(콘솔)을 통해 정책을 관리하기 시작한다. 실무 환경에서는 이 중앙 포털을 통해 '개인정보가 포함된 파일' 등 데이터 유형별로 정책을 정의하고, 이를 사용자 그룹별로 차등 적용(예시: '인사팀'은 예외, '개발팀'은 탐지)하며, 위반 시 수행할 행동(예시: 알림, 차단)을 정의하는 등 일관된 정책 배포가 가능해진다.

✓ **DLP 솔루션이 모니터링 모드로 동작하는가?**

- 실제 차단은 수행하지 않고 탐지 및 로깅 중심으로 운영되어 업무 영향도를 최소화한다.

■ **향상**

✓ **DLP 시스템이 전체적으로 도입되어 실시간으로 데이터를 보호하고 유출을 방지하는가?**

- 데이터 손실 방지(DLP) 기능이 전사적으로 도입되어, 실시간으로 데이터를 보호하고 유출을 방지한다. 실무 환경에서는 영역별 데이터 손실 방지(DLP)를 구현하여, 엔드포인트 영역은 별도 eDLP 시스템을 통해서(예시: 매체제어, 로컬 파일 암호화), 네트워크 영역은 ZTNA 게이트웨이를 통해서(예시: 내부망 전송 데이터 검사), 웹/클라우드 영역은 RBI 시스템이나 CASB, CANPP 시스템 등을 통해서(예시: 웹 업로드 차단, 클라우드 공유 통제) DLP 기능을 구현한다. 이러한 DLP 시스템들이 SIEM/SOAR, ICAM, EDR, eDRM 등 타 보안 시스템과 연동되어 정교한 정책을 통합 수행하며, 모든 주요 시스템 및 엔드포인트에 DLP 에이전트/정책이 적용되어 즉각적인 차단 및 알림이 가능하다.

✓ **DLP 솔루션이 방지 모드로 사용되는가?**

- '모니터링 모드'에서 '방지 모드(차단 모드)'로 전환하여 DLP 정책을 운영한다. 실무 환경에서는 eDLP, 네트워크 DLP, RBI 등이 데이터 거버넌스에서 정의된 데이터 카탈로그나 데이터 라벨링과 연동되어, '기밀' 또는 '개인정보'로 식별된 특정 민감 정보가 외부로 전송되거나, 복사/붙여넣기, 화면 캡처, USB 이동 등을 시도할 경우, 이를 즉각적으로 차단하거나 강제 암호화하는 등의 능동적인 조치를 수행한다.

■ **최적화**

✓ **DLP 시스템에 AI를 적용하여 데이터 유출 위험을 실시간으로 예측하고 차단할 수 있는가?**

- ML/AI 기반의 UEBA 기능이 전사적 데이터 손실 방지(DLP) 체계에 통합된다. 실무 환경에서는 SIEM/SOAR, eDLP, ZTNA 등에서 수집된 사용자 행동 패턴(예시: 평소와 다른 시간대의 대량 민감 데이터 접근, 비정상적인 외부 전송 시도)을 AI 엔진이 실시간으로 분석한다. 이를 통해 '향상' 단계의 정책 위반 탐지를 넘어, 실제 유출이 발생하기 전에 '유출 위험'을 예측하고, 이 예측(위험 점수)을

중앙 정책 엔진(PDP)(예시: ICAM)과 연동하여 해당 사용자의 세션을 선제적으로 차단하거나 격리하는 등 자동화된 대응을 수행한다.

✓ **변화하는 데이터 환경에 맞춰 자동으로 보안 정책이 최적화되는가?**

- 데이터 탐지-분류-차단/경고-보고-정책 조정에 이르는 DLP 운영의 전체 사이클(Lifecycle)이 자동화된다. 실무 환경에서는 ML/AI 기반의 DSPM 시스템이나 인하우스(In-house) 형태로 개발된 데이터 통합 관리 포털 등에서 데이터 카탈로그가 지속적으로 데이터 환경을 스캔하여, 신규 클라우드 앱(SaaS)이나 새로운 민감 데이터 패턴(예시: 신규 프로젝트 기밀정보)의 등장을 자동으로 식별한다. 이 정보는 중앙 정책 엔진(PDP)과 SIEM/SOAR에 연동되어, ML/AI 기반의 실시간 학습을 통해 기존 DLP 정책을 자동으로 갱신(최적화)하고, 관리자 승인 없이도 새로운 유출 경로와 민감 패턴에 대한 탐지 및 차단 정책이 자율적으로 적용된다.

항목	6.5.2 데이터 모니터링 및 감지	
설명	데이터 사용과 이동을 실시간으로 모니터링하고, 비정상적인 활동을 탐지하여 보안을 유지하는 과정이다. 데이터 소유자는 데이터 자산의 접근, 공유, 변환 및 사용에 대한 정보가 포함된 활성 메타데이터를 모니터링한다. DLP(데이터 손실 방지) 및 DRM(데이터 권한 관리) 적용 지점 분석을 수행하여 분석 도구를 배포할 위치를 결정한다. 파일 공유, 데이터베이스 등 DLP 및 DRM 범위 밖의 데이터는 대체 도구를 사용하여 변칙적이고 악의적인 활동이 있는지 적극적으로 모니터링하여야 한다.	
성숙단계	기존	데이터 활동을 수동으로 모니터링하고, 이벤트를 수동으로 기록하는가?
		데이터 모니터링 및 감지 프로세스가 수립되어 있는가?
	초기	자동화된 모니터링 도구를 통하여 데이터 활동을 감시할 수 있는가?
		모니터링 결과를 기반으로 보안 정책 조정이 가능한가?
	향상	데이터 활동을 분석하고 이상 징후를 실시간으로 탐지 가능한가?
		데이터 모니터링 결과를 다른 보안 시스템과 연계하여, 종합적인 보안 대응이 가능한가?
	최적화	모든 데이터 활동을 지속적으로 평가하고, 컨텍스트 기반 접근에 따라 최소 접근제어가 가능한가?

세부 설명

■ 기존

✓ **데이터 활동을 수동으로 모니터링하고, 이벤트를 수동으로 기록하는가?**

- 데이터 활동에 대한 모니터링이 자동화된 시스템(예시: SIEM) 없이, IT 관리자나 보안 담당자가 개별 시스템에 직접 접속하여 로그를 확인하는 등 수동으로 이루어진다. 실무 환경에서는 장애 발생이나 감사 요청 시에만 파일 서버 접근 로그, DB 로그 등을 수동으로 검토하고, CSV 또는 엑셀 파일 형태로 보안 이벤트를 별도 기록하여 관리하는 수준에 머무른다.

✓ **데이터 모니터링 및 감지 프로세스가 수립되어 있는가?**

- 데이터 모니터링 및 감지 프로세스가 기술적인 시스템보다는 관리적 절차에 의존한다. 실무 환경에서는 내부 보안 정책이나 IT 운영 매뉴얼 수준에서 '월 1회 DB 접근 로그 점검'과 같이 감시 항목과 주기를 정의하고 문서화한다. 이는 실시간 감지가 아닌, 사후 점검 및 감사(Audit) 목적의 프로세스에 해당한다.

■ 초기

✓ **자동화된 모니터링 도구를 통하여 데이터 활동을 감시할 수 있는가?**

- '기존' 단계의 수동 로그 검토에서 벗어나, SIEM(보안 정보 및 이벤트 관리)이나 중앙 로그 수집 도구를 바탕으로 데이터 활동을 감시하기 시작한다. 실무 환경에서는 eDLP, eDRM, DB 접근제어, 파일 서버 등에서 발생하는 데이터 이동, 접근, 변경, 삭제 관련 로그를 SIEM으로 자동으로 수집하고, 사전에 정의된 기본 규칙(Rule) 기반으로 분석(상관 분석)한다.

✓ **모니터링 결과를 기반으로 보안 정책 조정이 가능한가?**

- 모니터링 결과를 기반으로 기존 보안 정책을 조정하기 시작한다. 실무 환경에서는 SIEM에서 '비정상적인 대량 다운로드 시도'나 '평소와 다른 시간대 민감 데이터 접근' 등 사전에 정의된 이상 패턴이 탐지되면, 관리자가 이 경보(Alert)를 분석한다. 분석 결과를 바탕으로, eDLP나 DB 접근제어, eDRM 등의 정책을 수동으로 조정(예시: 해당 사용자의 다운로드 임계치 하향, 접근 시간 제한)하여 보안 정책을 개선하는 초기 수준의 피드백 루프를 운영한다.

■ **향상**

✓ **데이터 활동을 분석하고 이상 징후를 실시간으로 탐지 가능한가?**

- ML/AI 기반의 UEBA 기능을 통해 사용자별 데이터 활동을 심층적으로 분석하고 이상 징후를 실시간으로 탐지한다. 실무 환경에서는 SIEM, DSPM 또는 eDLP 시스템의 UEBA 기능이 파일 접근, 이동, 공유, 삭제 패턴 등을 학습하여 정상 행위 기준선(Baseline)을 수립한다. 이후, 이 기준선을 벗어나는 비정상적인 행동(예시: 평소와 다른 대량의 민감 파일 접근, 휴면 계정의 데이터 반출 시도)을 실시간으로 식별하고 즉각적인 경보를 제공하고 부분적으로 자동화 조치를 수행한다.

✓ **데이터 모니터링 결과를 다른 보안 시스템과 연계하여, 종합적인 보안 대응이 가능한가?**

- 데이터 모니터링 결과를 개별 시스템(예시: DB 접근제어 로그)에서만 확인하는 것이 아니라, 다른 보안 시스템과 연계하여 종합적인 보안 대응 체계를 구축한다. 실무 환경에서는 데이터 모니터링 결과(예시: DSPM의 민감 데이터 접근 탐지)를 SIEM으로 전송하여 EDR, eDLP, eDRM, ICAM 로그 등과 연관 분석을 수행한다. 나아가, 탐지된 위협을 보안 자동화 도구(SOAR)와 연동하여, 사전에 정의된 플레이북(Playbook)에 따라 '해당 계정 임시 잠금' 또는 'eDRM 권한 회수' 등의 대응 절차를 자동화한다.

■ **최적화**

✓ **모든 데이터 활동을 지속적으로 평가하고, 컨텍스트 기반 접근에 따라 최소 접근제어가 가능한가?**

- 모든 데이터 활동을 지속적으로 평가하고, 실시간 컨텍스트를 기반으로 최소 접근제어를 수행한다. 실무 환경에서는 이상 징후 탐지에서 확장되어, 중앙 정책 엔진(PDP)(예시: ICAM)이 사용자 위치, 시간, 기기 보안 상태 등 모든 컨텍스트를 실시간으로 평가하여 데이터 접근을 조건부로 허용(예시: JIT/JEA 기반의 최소 권한)하거나 자동으로 제한한다. 또한, AI 기반 분석을 통해 데이터 흐름을 학습하고 예측되는 위협(예시: 내부자 정보 유출 징후)을 사전에 탐지하며, SOAR 등과 연동하여 관련 차단 규칙(예시: eDLP, eDRM, PAM 정책)을 자동으로 생성하고, 우선순위 및 고위험 사용자를 중심으로 감시 리소스를 자동 분배하는 등 자율적인 데이터 모니터링 및 감지 체계를 운영한다.

7. 가시성 및 분석

항목	7.1 모든 관련 활동 기록	
설명	네트워크, 사용자, 기기, 애플리케이션 등에서 발생하는 모든 이벤트를 기록하고 저장하는 기능이다. 이는 로그 데이터를 생성하고, 이를 기반으로 향후 분석을 위한 데이터를 축적하는 역할을 한다. 관련 활동에는 로그인 시도, 접근권한 변경, 데이터 전송, 애플리케이션 실행 등 보안과 관련된 모든 행동이 포함된다. 이 기능은 잠재적인 보안 위협을 식별하고, 사건 발생 시 정확한 추적과 분석을 가능하게 한다.	
성숙단계	기존	로그 기록을 수동으로 수행하는가?
		로그 데이터가 특정한 시스템에서만 수집되는가?
	초기	다양한 시스템에서 자동으로 로그를 수집하는가?
		로그 수집 및 관리가 자동화되었는가?
	향상	수집된 데이터를 분석하여 보안 위협을 실시간으로 탐지 가능한가?
		로그 기록의 무결성을 보장하는가?
		로그 데이터를 기반으로 예측 분석(향후 발생한 위협 분석)이 가능한가?
	최적화	로그를 기반으로 자율 보안 체계가 구축되었는가?
		로그 항목을 자동으로 포맷을 맞추고 정규화가 가능한가?
		로그 분석을 통해 보안 정책이 자동으로 조정되는가?

세부 설명

■ **기존**

✓ **로그 기록을 수동으로 수행하는가?**

- 시스템, 네트워크, 애플리케이션 등에서 발생하는 다양한 이벤트와 보안 관련 활동에 대한 로그가 중앙 시스템(예시: 통합로그 시스템, SIEM)으로 자동 전송되지 않고, 담당자가 직접 확인하는 단계이다. 실무 환경에서는 장애 발생이나 감사 요청 시, 담당자가 개별 시스템 콘솔에 접속해 로그 파일을 수동으로 추출하고, 이를 엑셀, 워드, 메모장 등 문서 형태로 별도 관리한다. 이로 인해 로그 수집 및 저장이 자동화되어 있지 않아 실시간 분석이 불가능한 상태이다.

✓ **로그 데이터가 특정한 시스템에서만 수집되는가?**

- 로그 데이터가 중앙으로 통합되지 않고, 조직 내 일부 핵심 시스템(예시: 방화벽, 서버, 주요 애플리케이션)에서만 개별적으로 수집·관리되는 단계이다. 실무 환경에서는 다양한 네트워크 장비, 클라우드 서비스, Directory 인증 로그 등 전체 인프라에 대한 로그가 통합적으로 수집되지 않는다. 이로 인해 이벤트 분석이 개별 시스템 단위로만 수행되어, 전체적인 위협 상황을 파악하거나 상관관계 분석을 수행하기 어렵다.

■ **초기**

✓ **다양한 시스템에서 자동으로 로그를 수집하는가?**

- 개별 시스템에서 로그를 수집하고 분석하는 단계에서 확장되어 통합로그 시스템이나 SIEM 등을 도입하여 다양한 시스템의 로그를 자동으로 수집하기 시작한다. 실무 환경에서는 네트워크 장비, 서버, Directory 인증 로그, 클라우드 등 다양한 인프라에 설치된 에이전트 또는 Syslog 등을 통해 다양한 인프라에 대한 보안 관련 로그 및 이벤트 로그가 자동으로 중앙 저장소에 수집되는 단계를 의미한다.

✓ **로그 수집 및 관리가 자동화 되었는가?**

- 로그의 중앙집중화 및 자동 수집은 SIEM 등을 통해 수행되나, 로그 분석은 주로 수동으로 진행되거나 일부 자동화만 도입된 수준이다. 실무 환경에서는 수집된 로그가 주로 감사(Audit) 대응이나 장애 발생 시 사후 분석을 위해 저장되며, 통합로그 시스템이나 SIEM 등이 도입되었더라도 실시간 상관관계 분석 규칙(Rule)이 정교하지 않고, UEBA와 같은 고급 분석 기능이 부재하다. 이로 인해 로그 분석은 관리자가 수집된 로그에서 키워드 검색에 의존하는 경우가 많으며, 다양한 로그 유형 간의 상관관계 분석이나 실시간 위협 탐지는 제한적인 단계로 보안 가시성의 기반을 마련하는 단계에 해당한다.

■ **향상**

✓ **수집된 데이터를 분석하여 보안 위협을 실시간으로 탐지 가능한가?**

- 통합로그 시스템과 SIEM을 통해 중앙에 수집된 로그를 UEBA 기능과 연계하여 실시간으로 분석한다. 실무 환경에서는 사전에 정의된 상관관계 규칙에 기반하여(예시: VPN 로그인 성공 후 10분 이내 대량의 파일 접근 시도)와 같이 단일 로그로는 탐지하기 어려운 복합적인 보안 위협을 실시간으로 탐지하고 즉시 경고를 생성하여 관리자의 신속한 대응을 가능하게 한다.

✓ **로그 기록의 무결성을 보장하는가?**

- 로그 데이터의 위·변조를 방지하여 분석 결과의 신뢰성을 확보한다. 실무 환경에서는 로그 저장 시 암호화 및 해시를 적용해 소산 백업하거나, WORM(Write Once Read Many) 스토리지에 원본 로그를 저장해 로그 전송 시 해시값을 함께 전송하여 무결성을 검증하는 등, 위·변조 방지 및 감사 추적성 확보를 위한 기술적 조치가 이루어진 상태이다.

✓ **로그 데이터를 기반으로 예측 분석(향후 발생한 위협 분석)이 가능한가?**

- 과거 데이터와 행동 패턴을 바탕으로 머신러닝(ML) 등 고급 분석 기술을 활용하여 이상 징후나 잠재적 위협을 사전에 감지하기 시작한다. 실무 환경에서는 UEBA 시스템이 사용자의 정상 행위 기준선(Baseline)을 학습하고, 이를 벗어나는 통계적 이상 징후를 탐지하여 공격이 본격화되기 전에 선제적으로 대응할 수 있도록 지원한다.

■ **최적화**

✓ **로그를 기반으로 자율 보안 체계가 구축되었는가?**

- ML/AI 기술을 활용하여 모든 핵심 요소의 로그 데이터를 실시간으로 분석·학습하며, SIEM/SOAR 및 UEBA 기능과 유기적으로 연동된다. 실무 환경에서는 AI 엔진이 이상 행위(예시: 이상 로그인 시도, 비정상 트래픽 패턴 등)을 실시간 탐지하는 것을 넘어, 탐지된 위협에 따라 중앙 정책 엔진(ICAM 등)과 SOAR 플레이북 연계를 통해 정책시행지점(PEP)에 자동화된 대응(예시 :방화벽 규칙 추가, 사용자 접근

차단 등)을 즉각 수행한다. 또한, 과거 로그 데이터를 학습하여 제로데이(Zero-Day) 공격과 같은 알려지지 않은 위협까지 사전 예측하는 자율 보안 체계가 구축된 상태이다.

✓ **로그 항목을 자동으로 포맷을 맞추고 정규화가 가능한가?**

- 이기종 시스템에서 수집된 비정형 로그를 SIEM이나 빅데이터 플랫폼에서 자동으로 정규화한다. 실무 환경에서는 AI 어시스턴트 기능이 비정형 로그 샘플을 분석하여 최적의 파싱(Parsing) 규칙과 정규 표현식을 자동 생성하고, 이를 공통된 포맷(예시: CEF, LEEF)으로 표준화하여 분석 효율성을 극대화한다.

✓ **로그 분석을 통해 보안 정책이 자동으로 조정되는가?**

- 그 분석 결과가 정책결정지점(PDP)(예시: ICAM)의 동적 리스크 스코어링에 실시간으로 반영되어 보안 정책이 자동으로 조정된다. 실무 환경에서는 UEBA 기능을 통해 분석한 사용자/기기 위험 점수가 높을 경우, PDP가 이를 즉시 인지하여 접근권한을 제한하도록 정책을 결정한다. 이 결정은 정책시행지점(PEP)(예시: ZTNA, PAM, 마이크로 세그멘테이션 등)으로 전달되어 해당 사용자의 세션을 강제 종료하거나 MFA를 요구하는 등 리스크 기반 접근제어가 자동으로 수행된다. 또한 AI가 트래픽 패턴 변화를 감지해 보안 정책을 동적으로 업데이트하거나, 정책 변경 전 잠재적 영향을 평가하는 시뮬레이션까지 수행하는 자율적인 정책 순환 체계가 완성된다.

항목	7.2 중앙집중적 보안 정보 및 이벤트 관리	
설명	중앙화된 SIEM은 다양한 보안 이벤트 및 로그 데이터를 한 곳에서 수집하고 관리하는 시스템이다. SIEM은 다수의 보안 도구에서 데이터를 통합하여, 실시간 모니터링, 로그 분석, 경고 및 보고서 작성 기능을 제공한다. 이를 통해 네트워크 전체의 보안 상태를 중앙에서 파악하고, 빠르게 보안 사고에 대응할 수 있다. SIEM은 보안 정책 준수 및 규제 요구사항을 충족하는데 도움을 준다.	
성숙단계	기존	보안 이벤트가 발생하면 수동으로 데이터를 분석하는가?
	초기	SIEM 시스템이 도입되었는가?
		중앙집중적 보안 관리 체계가 구축되었는가?
	향상	SIEM 시스템은 다양한 보안 도구와 연동되어 보안 데이터를 종합적으로 분석하는가?
	최적화	AI 기반으로 보안 이벤트를 분석하는가?
		비정상적인 활동에 대하여 자동 대응이 가능한가?

세부 설명

■ **기존**

✓ **보안 이벤트가 발생하면 수동으로 데이터를 분석하는가?**

- 보안 이벤트 발생 시 데이터를 중앙에서 통합적으로 관리하지 않고, 각 시스템에서 발생하는 보안 기록을 개별적으로 수집·관리하는 단계로, 각 시스템에서 발생하는 로그가 서로 다른 포맷으로 저장되며, 보안 사고가 발생할 경우 관련 시스템의 로그를 일일이 수집해 스프레드시트나 문서로 정리한다. 수집된 로그를 기반으로 담당자가 직접 이상 징후를 찾아내고 대응하는 상태이다.

■ **초기**

✓ **SIEM 시스템이 도입되었는가?**

- '기존' 단계의 수동 로그 취합에서 확장되어, SIEM이 도입되고 로그의 수집, 저장, 관리가 자동화된 상태이다. 실무 환경에서는 네트워크 장비(예시: 방화벽 로그, Directory 인증 로그, 보안장비 이벤트 로그 등) 다양한 인프라의 로그가 SIEM 시스템으로 실시간 전송되어 중앙에서 관리된다.

✓ **중앙집중적 보안 관리 체계가 구축되었는가?**

- 각 시스템에서 분산 관리되던 보안 로그가 SIEM에서 통합되어, 전체적인 보안 상태를 중앙집중 시스템(예시: SIEM 관리콘솔, 정보보안포털 연계 등)을 통해 파악하는 것이 가능하다. 실무 환경에서는 보안 사고 발생 시, 중앙 SIEM에서 관련 로그를 신속하게 추적하고 사전에 정의된 정적 규칙(Static Rule) 기반의 상관 분석을 수행할 수 있는 기반이 마련된 상태이다.

■ **향상**

✓ **SIEM 시스템은 다양한 보안 도구와 연동되어 보안 데이터를 종합적으로 분석하는가?**

- SIEM이 다양한 보안 도구(예시: EDR, NDR, PAM, ZTNA, ICAM 등)와 연동되어 보안 데이터를 종합적으로 분석하는 단계이다. 실무 환경에서는 SIEM 구성하는 예시로는 라이선스 비용 및 성능을 고려하여, 모든 원본 로그는 통합로그 시스템이나 빅데이터 플랫폼에 저장하고, SIEM으로는 상관 분석에 필요한 핵심 이벤트 로그만 선별적으로 전송하여 분석을 수행한다. 또한, SIEM 자체의 UEBA 기능을 활용하거나 UEBA 전용 시스템과 연동하여, 사용자 및 기기의 이상 징후를 탐지하고 분석한다. 탐지된 위협은 사전에 정의된 워크플로우에 따라 보안 운영팀에 알림을 제공하거나, SOAR 시스템과 연동하여 자동화된 대응 조치를 실행할 수 있다.

■ **최적화**

✓ **AI 기반으로 보안 이벤트를 분석하는가?**

- ML/AI 기반의 UEBA 기능이 SIEM 및 빅데이터 플랫폼과 통합되어, 발생하는 모든 로그와 이벤트를 실시간으로 수집·분석한다. 실무 환경에서는 AI 엔진이 사용자 및 기기의 행동 패턴을 학습하고 이벤트(예시: EDR에서 탐지된 의심스러운 프로세스 실행과 NDR에서 탐지된 외부 C&C 통신 시도를 연계) 간의 연결성을 분석하여, 단일 이벤트로는 파악하기 어려운 복합 공격 시나리오를 구성한다. 이 분석 결과는 '위협'으로 규정되어 정책결정지점(PDP)(예시: ICAM)으로 전달, 동적 리스크 스코어링의 근거로 사용된다.

✓ **비정상적인 활동에 대하여 자동 대응이 가능한가?**

- 탐지된 위협과 정책결정지점(PDP)(예시: ICAM)에서 산출된 동적 리스크 스코어에 기반하여 자동화된 대응을 실행한다. 실무 환경에서는 PDP가 고위험으로 판단할 경우, 정책시행지점(PEP)(예시: ZTNA, PAM, 마이크로 세그멘테이션)에 직접 정책을 전달하여 동적 정책 조정(예시: '읽기 전용' 권한으로 강제 하향)이나 '세션 강제 종료' 등의 대응을 수행할 수 있다. 또한, 더 복잡한 대응이 필요할 경우 PDP가 SOAR와 연계하여, SOAR 플레이북을 통해 다양한 보안 솔루션에 해당하는 정책시행지점(PEP)에 '사용자 계정 잠금' 또는 '기기 격리' 등 자율적인 대응을 수행하도록 한다.

항목	7.3 보안 위협 분석	
설명	네트워크에서 발생하는 다양한 활동 및 로그를 분석하여, 잠재적인 보안 위협을 식별하고 대응하는 기능이다. 이는 수집된 로그와 데이터를 기반으로 공격 패턴, 취약점, 이상 행동 등을 분석하여 위협을 사전에 탐지하고, 필요 시 자동으로 조치를 취하는데 사용된다. 보안 위협 분석은 실시간으로 수행되며, 침입 시도나 악성 활동을 빠르게 파악하여 피해를 최소화할 수 있다.	
성숙단계	기존	보안 로그 및 데이터를 수동으로 수집하는가?
		CVE, ExploitDB 등의 취약점을 수동으로 수집하는가?
	초기	알려진 취약점에 대한 평가 기준을 마련하였는가?
		수집된 취약점에 대한 경고가 자동으로 이루어지는가?
	향상	자동화된 보안 위협 분석 도구를 도입하였는가?
		실시간 보안 위협 탐지가 가능한가?
	최적화	AI 기반 예측 분석 시스템을 통하여 위협에 대한 예측이 가능한가?

세부 설명

■ 기존

✓ 보안 로그 및 데이터를 수동으로 수집하는가?

- 보안 로그와 데이터를 자동화된 시스템 없이 담당자가 각 시스템에서 직접 추출하는 단계이다. 로그 파일이나 이벤트 데이터를 일일이 확인하고, 필요한 정보를 수동으로 복사하거나 별도의 문서(엑셀, 워드 등)에 정리하고, 로그와 보안 데이터가 여러 시스템에 분산 저장되어 있어 통합관리 체계가 부재하며, 보안 이벤트 발생 시 각 시스템에 접속해 데이터를 개별적으로 수집해야 하는 상태이다.

✓ CVE, ExploitDB 등의 취약점을 수동으로 수집하는가?

- 최신 보안 취약점 정보(CVE, ExploitDB 등)를 자동화된 CTI(사이버 위협 인텔리전스) 피드(Feed) 없이 담당자가 직접 확인하고, 필요한 정보를 수동으로 검색하여 취합한다. 실무 환경에서는 보안 담당자가 공식 웹사이트, 데이터베이스, 보안 커뮤니티 등을 직접 방문해 취약점 정보를 수집하고, 이를 내부 문서로 정리하거나 각 시스템에 수동 반영한다.

■ 초기

✓ 알려진 취약점에 대한 평가 기준을 마련하였는가?

- 알려진 취약점에 대한 평가 기준을 CVSS(Common Vulnerability Scoring System)와 같은 표준 평가 프레임워크를 기반으로 수립하여 내부 정책으로 관리한다. 실무 환경에서는 이 기준을 활용하여 수집된 취약점의 위험 등급(예시: 'High', 'Medium', 'Low')을 분류하고 대응 우선순위를 정의하는 단계를 의미한다.

✓ **수집된 취약점에 대한 경고가 자동으로 이루어지는가?**

- 수집된 취약점 정보에 대해 기본적인 자동화가 구현된 상태이다. 실무 환경에서는 SIEM에 CTI 정보를 연동하거나 별도 피드 수신 시스템, 또는 취약점 관리 시스템이 CVSS 점수 'High' 등급 이상의 취약점을 탐지하면, IT팀과 보안팀에 이메일이나 메신저로 경고가 자동으로 전송된다. 이 단계의 자동화는 위협 대응(Response)보다는 위협 탐지 및 통보(Alert)에 중점을 둔다.

■ **향상**

✓ **자동화된 보안 위협 분석 도구를 도입하였는가?**

- SIEM/SOAR, 빅데이터 플랫폼, XDR 등 자동화된 보안 위협 분석 도구를 도입하여, 네트워크, 엔드포인트, 클라우드 등 다양한 환경에서 수집된 로그와 이벤트를 자동으로 상관관계 분석한다. 실무 환경에서는 UEBA 기능을 활용해 사용자 및 기기의 정상 행동 패턴 기준선(Baseline)을 학습하고, 이 기준선에서 벗어나는 편차가 발생 시 자동으로 경고를 생성하고 대응한다.

✓ **실시간 보안 위협 탐지가 가능한가?**

- 수집된 로그와 이벤트 데이터를 기반으로, 실시간 보안 위협 탐지가 가능한 통합 분석 체계가 구축된 상태이다. 실무 환경에서는 외부 CTI 정보를 SIEM이나 XDR 등과 연동하여, 신규 위협(예시: 악성 IP, C&C 서버) 정보를 분석 규칙에 자동으로 반영(적용)한다. 또한, UEBA 기능으로 탐지한 내부 이상 징후(예시: 평소와 다른 시간대의 대량 접근)까지 실시간으로 탐지한다. 이러한 실시간 위협 탐지 및 대응 체계는 내부 SOC(보안 운영 센터) 조직, MDR(Managed Detection and Response)과 같은 전문 관제 서비스(외주), 또는 내부 인력과 외주 인력이 협업하는 하이브리드 모델을 통해 운영될 수 있다. 탐지된 결과는 R&R(역할 및 책임)에 따라 즉시 관리자에게 경고되거나 SOAR 시스템으로 전달되어 대응 프로세스가 운영된다.

■ **최적화**

✓ **AI 기반 예측 분석 시스템을 통하여 위협에 대한 예측이 가능한가?**

- ML/AI 엔진이 SIEM, 빅데이터 플랫폼, XDR 등에서 수집된 방대한 데이터를 실시간으로 분석한다. 실무 환경에서는 UEBA 기능이 사용자와 디바이스의 정상 패턴과의 편차를 즉시 탐지하고, CTI 정보와 연계하여 알려지지 않은 위협이나 잠재적 공격(예시: 제로데이 공격 징후)을 조기에 예측하고 경고한다. 해당 예측 분석 결과는 정책결정지점(PDP)(예시: ICAM)의 동적 리스크 스코어링에 반영되어 보안 정책이 자동으로 조정되며, 위험도가 높은 상황에서는 PDP가 정책시행지점(PEP)(예시: ZTNA, PAM)에 직접 정책을 전달하거나 SOAR와 연동하여 '즉시 차단', '기기 격리', '추가 인증' 등 자동화된 대응이 이어진다. 또한 AI 엔진이 과거 사건과 새로운 데이터를 지속적으로 학습하여 탐지 정확도와 대응 속도를 향상시키며, 변화하는 위협 환경에 맞춰 자율적으로 보안 체계를 최적화한다.

항목	7.4 사용자 및 기기 동작 분석	
설명	네트워크 내의 사용자의 행동 패턴과 기기활동을 모니터링하여, 비정상적이거나 의심스러운 활동을 탐지하는 기능이다. 이를 통해 정상적인 행동과 이상 행동을 구분하고, 악의적인 활동을 탐지할 수 있다. 예를 들어, 평소와 다른 시간에 접속하거나, 특정 사용자가 비정상적으로 많은 데이터를 전송할 경우 이를 탐지하여 경고를 발송할 수 있다. 이 기능은 AI 및 머신러닝을 활용하여 행동 패턴을 학습하고, 실시간으로 분석을 수행한다.	
성숙단계	기존	사용자와 기기의 기본적인 활동 데이터를 수집하는가?
		비정상 행동을 수동으로 탐지하는가?
		기본적인 사용자 행동 패턴을 기록하고, 의심스러운 활동을 발견하면 이를 추적하는가?
	초기	자동화된 사용자 및 기기 동작 분석 도구를 도입하였는가?
		사용자의 행동 패턴과 기기의 활동을 자동으로 분석하는가?
	향상	행동 분석 기능을 도입하여 비정상적인 사용자 활동과 기기 동작을 탐지하는가?
		AI 기반으로 사용자 및 기기의 행동 패턴을 학습하고, 지속적으로 변화하는 패턴에 따라 실시간으로 대응 가능한가?
	최적화	사용자 및 기기 동작에 대하여 비정상 행위를 자동으로 파악하여 보안 정책을 자동으로 조정하고 최소 권한을 부여할 수 있는가?

세부 설명

■ **기존**

✓ **사용자와 기기의 기본적인 활동 데이터를 수집하는가?**

- 사용자와 기기의 기본적인 활동 데이터가 중앙에서 분석되지 않고, 개별 시스템(예시: 서버 접속 로그, 방화벽 로그)에서 수동으로 취합되는 단계이다. 실무 환경에서는 네트워크, 시스템, 애플리케이션 등에서 발생하는 로그인, 접속 시간, IP 주소, 간단한 활동 기록 등 단순한 활동 데이터만을 수동 또는 단순 로그 수집 시스템을 통해 취합한다.

✓ **비정상 행동을 수동으로 탐지하는가?**

- 비정상적인 사용자 또는 기기 행동은 주로 담당자가 로그를 직접 확인하거나, 주기적으로 수집된 데이터를 검토하여 수동으로 탐지한다. 자동화된 이상 징후 탐지 도구가 도입되어 있지 않아, 의심스러운 활동을 발견하려면 담당자의 경험과 직관에 의존하는 경우가 많은 상태이다.

✓ **기본적인 사용자 행동 패턴을 기록하고, 의심스러운 활동을 발견하면 이를 추적하는가?**

- 사용자 및 기기의 기본적인 행동 패턴은 개별 시스템에 로그 형태로 기록되나, 이는 주로 단순 저장 및 통계용으로만 사용된다. 실무 환경에서는 의심스러운 활동이 발견되더라도(예시: 특정 계정의 잦은 로그인 실패), 해당 로그를 SIEM 등과 연계하여 자동으로 추적하거나 분석하지 못하고, 담당자가 수동으로 관련 시스템의 로그를 일일이 추적하여 확인한다.

■ **초기**

✓ **자동화된 사용자 및 기기 동작 분석 도구를 도입하였는가?**

- 자동화된 사용자 및 기기 동작 분석 도구를 도입하기 시작한다. 실무 환경에서는 SIEM의 기본적인 상관관계 분석 기능이나, EDR, NAC(ZTNA) 등 개별 솔루션에서 제공하는 초기 수준의 이상 행위 탐지 기능을 활용한다. 이를 통해 각 시스템에 설치된 에이전트 또는 중앙 로그 수집기를 통해 사용자와 기기의 활동 정보를 자동으로 취합하며, 네트워크 내 모든 활동을 실시간으로 모니터링하기 시작한다.

✓ **사용자의 행동 패턴과 기기의 활동을 자동으로 분석하는가?**

- 도입된 분석 도구는 주로 정적 규칙(Static Rule)에 기반하여 사용자 행동 패턴과 기기 활동을 자동으로 분석한다. 실무 환경에서는 SIEM에 설정된 '특정 시간 외 로그인 시도', '반복적인 로그인 실패' 등과 같은 사전에 정의된 시나리오에 따라 이상 징후나 비정상적인 활동이 감지된다. 이 경우, 시스템이 자동으로 경고(Alert)를 생성하여 관리자에게 알림을 전달하지만, ML/AI 기반의 동적인 기준선(Baseline) 분석은 미흡한 상태이다.

■ **향상**

✓ **행동 분석 기능을 도입하여 비정상적인 사용자 활동과 기기 동작을 탐지하는가?**

- 고급분석 기능에 해당하는 UEBA 기능이 도입되어, 사용자와 기기의 활동 데이터를 실시간으로 수집·분석한다. 실무 환경에서는 SIEM이나 XDR 등에서 수집된 로그를 기반으로 ML/AI 분석 엔진이 정상적인 행동 패턴 기준선(Baseline)을 학습하고, 비정상적인 사용자 활동(예시 :평소와 다른 시간·장소에서의 로그인, 비정상적인 대량 데이터 전송, 권한 상승 시도 등)이나, 의심스러운 기기 동작(예시: 미승인 기기 접속, 비정상 네트워크 트래픽)을 자동으로 탐지하여 경고를 생성한다.

✓ **AI 기반으로 사용자 및 기기의 행동 패턴을 학습하고, 지속적으로 변화하는 패턴에 따라 실시간으로 대응 가능한가?**

- ML/AI 기반 UEBA 기능이 사용자 및 기기의 행동 패턴을 지속적으로 학습하며, 변화하는 업무 환경과 새로운 위협에 따라 실시간으로 탐지·대응한다. 실무 환경에서는 행동 패턴의 변화가 감지되면 AI가 이를 자동으로 인지하고 정상/비정상 여부를 판단하여, 이 분석 결과를 정책결정지점(PDP)(예시: ICAM)에 전달하여 동적 리스크 스코어링에 반영한다. PDP는 이 스코어에 기반하여 정책시행지점(PEP)(예시: ZTNA, PAM)을 통해 '접근 제한', '추가 인증 요구', '세션 종료' 등 실시간 대응을 수행한다.

■ **최적화**

✓ **사용자 및 기기 동작에 대하여 비정상 행위를 자동으로 파악하여 보안 정책을 자동으로 조정하고 최소 권한을 부여할 수 있는가?**

- ML/AI 기반의 고도화된 UEBA 기능이 SIEM, XDR 등에서 수집된 로그를 바탕으로 사용자 및 기기의 정상 행동 패턴을 지속적으로 학습한다. 실무 환경에서는 AI 엔진이 평소와 다른 비정상적인 활동을 실시간으로 탐지하고, 이 탐지 결과는 즉시 정책결정지점(PDP)(예시: ICAM)으로 전달되어 동적 리스크 스코어링에 반영되며, 탐지된 비정상 행위에 따라 보안 정책이 자동으로 조정된다. 또한, PDP는 이 분석 결과를 바탕으로 JIT/JEA 원칙을 적용하여, 각 사용자의 업무 환경과 실시간 행동 패턴에 따라 필요한 최소 권한만을 동적으로 자동 부여하고, 불필요한 권한은 자동으로 회수하는 자율적인 보안 체계를 의미한다.

항목	7.5 위협 인텔리전스 통합	
설명	외부의 보안 위협 정보를 수집하고 이를 조직 내 보안 시스템에 적용하여 위협 대응 능력을 향상시키는 기능이다. 위협 인텔리전스는 악성 IP 주소, 도메인, 취약점 정보 등 다양한 외부 데이터를 포함하며, 이를 통해 조직 내에서 발생할 수 있는 위협을 사전에 탐지하고 차단할 수 있다. 이 기능은 위협 데이터베이스와 연동되어 지속적으로 최신 정보를 업데이트하며, 보안 시스템과 통합되어 자동으로 대응 조치를 취할 수 있다.	
성숙단계	기존	외부의 보안 위협 정보를 수동으로 수집하는가?
		위협 데이터를 조직 내 시스템과 수동으로 연동하는가?
	초기	자동화된 위협 인텔리전스 통합 도구를 도입하였는가?
	향상	위협 인텔리전스를 내부 시스템과 통합하였는가?
	최적화	AI 기반의 위협 인텔리전스 시스템을 구축하였는가?

세부 설명

■ 기존

✓ 외부의 보안 위협 정보를 수동으로 수집하는가?

- 외부 위협 인텔리전스를 수집하는 자동화된 CTI(사이버 위협 인텔리전스) 플랫폼 없이, 보안 담당자가 공개 소스(OSINT), 보안 커뮤니티, 뉴스, 블로그 등을 직접 탐색하여 위협 정보를 수동으로 수집한다. 실무 환경에서는 주로 알려진 악성 IP, 도메인, 기본 공격 시그니처 등 단순한 IOC(침해 지표) 정보만 취합하며, 공격 그룹이나 TTPs(전술, 기술, 절차)와 같은 심층 분석 자료는 부재한 상태이다.

✓ 위협 데이터를 조직 내 시스템과 수동으로 연동하는가?

- 수집된 위협 데이터를 조직 내 보안 시스템에 수동으로 반영한다. 실무 환경에서는 담당자가 취합한 악성 IP 목록 등을 방화벽, IPS 등 개별 보안 시스템의 관리 콘솔에 직접 입력하여 차단 정책을 설정한다. SIEM이나 EDR 등 내부 시스템과의 자동 연동이 미구축되어 있어, 데이터 중복 입력 및 시스템 간 정책 불일치가 발생할 가능성이 있으며 실시간 대응이 어렵다.

■ 초기

✓ 자동화된 위협 인텔리전스 통합 도구를 도입하였는가?

- CTI(사이버 위협 인텔리전스) 플랫폼이나 TIP(위협 인텔리전스 플랫폼) 등 자동화된 위협 인텔리전스 통합 도구를 도입하여 외부 위협 데이터를 자동으로 수집·통합하기 시작한다. 실무 환경에서는 이러한 플랫폼이 SIEM 시스템과 API 기반 연동을 통해, 수집된 IOC(침해 지표)(예시: 악성 IP, 도메인, 알려진 악성 파일 해시) 데이터를 실시간으로 전송한다. SIEM은 이 정보를 받아 상관관계 규칙에 활용하며, 내부 로그에서 일치하는 항목이 발견되면(예시: 내부 기기가 알려진 악성 IP와 통신 시도) 자동으로 경고를 생성한다. 이 단계에서는 위협 정보가 주기적으로 자동 갱신되어 최신 위협 정보를 반영하는 것에 중점을 둔다.

■ 향상

✓ 위협 인텔리전스를 내부 시스템과 통합하였는가?

- SIEM에서 수집된 내부 보안 데이터(예시: 서버 이벤트 로그, EDR 탐지 이벤트 등)와 외부 위협 인텔리전스를 통합하여 분석한다. 실무 환경에서는 단순 IOC(침해 지표)(예시: 악성 IP, 도메인, 취약점 정보) 뿐만 아니라, 특정 공격 그룹의 TTPs(전술, 기술, 절차)를 심층 분석하여 내부 자산에 미칠 수 있는 실제 위협을 식별한다. 또한, 이 분석된 위협 정보는 정책결정지점(PDP)(예시: ICAM)의 리스크 스코어링에 반영되거나 SIEM/SOAR 시스템과 즉시 연동되어, 정책시행지점(PEP)(예시: NGFW, EDR, ZTNA)의 정책을 실시간으로 업데이트(예시: 관련 TTPs 탐지 규칙 자동 추가)하는 등 선제적인 방어 조치를 수행한다.

■ 최적화

✓ AI 기반의 위협 인텔리전스 시스템을 구축하였는가?

- 외부 위협 데이터를 실시간으로 수집·통합하는 것을 넘어 내부 보안 시스템(예시: SIEM, UEBA, XDR 등)의 이벤트와 결합하여 분석한다. 실무 환경에서는 AI 엔진이 과거 공격 데이터와 실시간 내/외부 위협 정보를 학습하여, 알려지지 않은 신규 위협이나 제로데이 공격을 사전에 예측한다. 이 예측 분석 결과와 내부 이벤트(예시: UEBA의 이상 징후)를 종합하여 정책결정지점(PDP)(예시: ICAM)에서 사용자 및 기기의 동적 리스크 스코어를 산출하며, 위험도가 높다고 판단될 경우 SOAR와 연동하거나 정책 시행지점(PEP)(예시: ZTNA, PAM)을 통해 '접근 제한', '추가 인증 요구', '세션 격리' 등 자율적인 동적 정책을 실행한다.

항목	7.6 자동화된 동적 정책	
설명	실시간으로 발생하는 보안 이벤트와 분석 결과를 기반으로 네트워크의 보안 정책을 자동으로 변경하는 기능이다. 이는 보안 위협이나 비정상적인 활동이 감지되었을 때, 사전에 정의된 정책을 자동으로 적용하거나 새로운 정책을 실시간으로 생성하여 네트워크 보안을 강화하는데 사용된다. 예를 들어, 특정 사용자의 행동이 이상하다고 판단되면 그 사용자의 접근권한을 자동으로 제한하거나, 네트워크 세그먼트를 재조정할 수 있다. 자동화된 동적 정책은 빠르고 유연한 대응을 가능하게 하여, 보안 사고를 최소화할 수 있다.	
성숙단계	기존	보안 정책을 수동으로 관리하는가?
		보안 이벤트가 발생할 경우 관리자가 직접 정책을 수정하여 대응하는가?
	초기	자동화된 정책 관리 시스템을 도입하였는가?
		보안 이벤트 발생 시 자동으로 정책을 변경하고 적용하는가?
	향상	동적 정책을 실시간으로 조정하여, 보안 이벤트 발생 시 즉각적으로 새로운 정책을 생성하고 적용하는가?
		위협 탐지와 연계하여 동적으로 정책을 조정하는가?
	최적화	AI 기반의 자동화된 동적 정책 시스템을 구축하여, 보안 이벤트 분석 결과에 따라 자율적으로 정책을 조정하는가?

세부 설명

■ **기존**

✓ **보안 정책을 수동으로 관리하는가?**

- 보안 정책이 문서(예시: 정보보호 정책/지침/절차서 등)로는 정의되어 있어 해당 정책을 기반으로 담당자가 수동으로 관리하는 단계이다. 실무 환경에서는 관리자가 방화벽, AV, NAC, PAM 등 개별 보안 솔루션에 직접 접속하여 정의된 보안 정책을 수동으로 적용한다. 또한, 주기적인 로그 분석이나 선제적인 정책 수정보다는, 장애가 발생하거나 특정 이벤트(예시: 신규 IP 허용 요청)가 발생했을 때만 정책을 사후에 수동으로 업데이트하는 정적인(Static) 정책 관리 상태를 의미한다.

✓ **보안 이벤트가 발생할 경우 관리자가 직접 정책을 수정하여 대응하는가?**

- 보안 이벤트(예시: 악성코드 탐지) 발생 시, 자동화된 동적 정책 조정이 불가능하여 관리자가 백신이나 취약점 점검 도구 로그 등을 수동 분석한 후, 회의를 통해 대응 방안(예시: 해당 IP 대역 차단)을 결정한다. 실무 환경에서는 이 결정 사항을 바탕으로 관리자가 다시 개별 보안 장비(예시: 방화벽, IPS 등)에 접속하여 수동으로 정책을 수정하며, 대응까지 상당한 시간이 소요되는 상태이다.

■ **초기**

✓ **자동화된 정책 관리 시스템을 도입하였는가?**

- 개별적으로 운영되던 보안 정책 관리 도구를 통합하여 중앙에서 관리하기 시작하는 단계이다. 실무 환경에서는 기존에 분리되어 있던 '시스템 접근제어'와 'DB 접근제어'를 PAM 시스템으로 통합하여

관리하거나, Directory 수준에서 관리되던 계정 관리를 IAM(통합계정권한관리)으로 확장하여 애플리케이션 접근 및 권한 신청을 통합 관리하는 것을 의미한다. 이러한 통합 정책은 정보보안 포털 등을 통해 중앙에서 일괄적으로 배포·적용되기 시작한다.

✓ **보안 이벤트 발생 시 자동으로 정책을 변경하고 적용하는가?**

- SIEM에서 보안 이벤트가 탐지되면, 사전에 정의된 시나리오 기반의 정적 조건(예시: 5분 내 10회 로그인 실패, 비인가 IP 접속 시도)에 따라 시스템이 자동으로 정책을 변경하거나 차단 규칙을 적용한다. 실무 환경에서는 SIEM이 SOAR의 간단한 플레이북을 호출하거나, 정책시행지점(PEP)과 직접 연동되어 '해당 IP 차단'과 같은 기본적인 자동화 정책을 적용하는 단계를 의미한다.

■ **향상**

✓ **동적 정책을 실시간으로 조정하여, 보안 이벤트 발생 시 즉각적으로 새로운 정책을 생성하고 적용하는가?**

- 정책 시스템이 고도화되어 SIEM이나 UEBA 시스템 등에서 이상 행위, 위협 탐지 등 보안 이벤트가 발생하면, 정책결정지점(PDP)(예시: ICAM, ZTNA 등)이 이를 실시간(예시: 10~60초 이내)으로 인지한다. 실무 환경에서는 PDP가 이 정보를 바탕으로 새로운 정책을 자동 생성·적용하여, 수동 개입 없이 복합 공격이나 다단계 위협에 신속하게 대응할 수 있다.

✓ **위협 탐지와 연계하여 동적으로 정책을 조정하는가?**

- SIEM/SOAR, EDR, XDR 등 위협 탐지 시스템과 정책결정지점(PDP)(예시: ICAM, ZTNA 등)이 연계되어, 위협 탐지 결과에 따라 정책을 실시간으로 동적으로 조정한다. 실무 환경에서는 SIEM에서 특정 공격 시그니처가 탐지되거나 UEBA가 이상 징후를 식별하면, 이 정보가 PDP로 전달된다. PDP는 이 정보를 바탕으로 리스크를 재평가하고, 정책시행지점(PEP)(예시: NGFW, ZTNA 게이트웨이, 마이크로 세그멘테이션 등)의 정책을 자동으로 강화(예시: 해당 IP/사용자의 접근 레벨 하향 조정)하여 추가 피해를 차단한다.

■ **최적화**

✓ **AI 기반의 자동화된 동적 정책 시스템을 구축하여, 보안 이벤트 분석 결과에 따라 자율적으로 정책을 조정하는가?**

- ML/AI 기반의 자율 정책 엔진인 정책결정지점(PDP)(예시: ICAM)이 도입되어, SIEM, UEBA, CTI 등에서 수집된 모든 보안 이벤트와 실시간 분석 결과에 따라 자율적으로 정책을 조정한다. 실무 환경에서는 AI 엔진이 네트워크 트래픽, 사용자·기기 행동 패턴 등을 지속적으로 학습하여, 정책 변경이 필요한 상황을 예측하거나(예시: 제로데이 공격 징후) 이상 징후를 탐지한다. 이 분석 결과는 PDP의 동적 리스크 스코어링에 즉시 반영되며, PDP는 탐지된 위협 수준에 따라 정책시행지점(PEP)(예시: ZTNA, 마이크로 세그멘테이션, NGFW)에 '접근권한 제한'이나 '세그먼트 격리' 정책을 직접 전달하거나, SOAR 플레이북과 연동하여 '추가 인증 요구' 등 다양한 정책을 자율적으로 적용한다.

8. 자동화 및 통합

항목	8.1 정책 통합	
설명	조직 내 보안 정책을 자동으로 조정하고, 여러 시스템과 네트워크 장비에 일관된 정책을 적용하는 프로세스이다. 보안 이벤트 발생 시 실시간으로 정책을 변경하거나 조정할 수 있으며, 이를 통해 신속하고 일관된 보안 대응이 가능해진다.	
성숙단계	기존	정책 조정 시 수동으로 각 시스템에 일일이 변경 사항을 반영하는가?
	초기	자동화된 정책 통합 시스템을 도입하여 보안 정책을 중앙에서 관리하는가?
		정책 변경이 자동으로 이루어지는가?
	향상	실시간 보안 이벤트를 기반으로 정책을 동적으로 조정하는가?
		위협에 따라 즉각적으로 정책을 수정하고 적용하는 자동화된 프로세스가 존재하는가?
	최적화	AI 기반의 자율 정책 통합 시스템을 통해, 상황에 맞게 정책을 자동으로 조정 가능한가?

세부 설명

■ **기존**

✓ **정책 조정 시 수동으로 각 시스템에 일일이 변경 사항을 반영하는가?**

- 보안 정책이 정보보안 포털 등 중앙 시스템을 통해 통합 관리되지 않고, 각 시스템별로 분산되어 수동으로 관리되는 단계이다. 실무 환경에서는 보안 정책(예시: 정보보호 정책/지침)이 문서로는 정의되어 있고, 사용자가 정책 변경(예시: 신규 IP 허용 요청)을 그룹웨어나 메일 등으로 요청하면 담당자가 방화벽, AV, NAC, PAM 등 개별 보안 솔루션에 직접 접속하여 일일이 변경 사항을 수동으로 적용한다. 이로 인해 시스템 간 정책이 상충되거나 누락될 수 있으며, 일관성 유지가 어려운 정적인(Static) 정책 관리 상태를 의미한다.

■ **초기**

✓ **자동화된 정책 통합 시스템을 도입하여 보안 정책을 중앙에서 관리하는가?**

- 개별적으로 운영되던 보안 정책 관리 도구를 핵심 요소(Pillar)별로 통합하여 중앙에서 관리하기 시작하는 단계이다. 실무 환경에서는 '시스템' 영역의 경우, 기존에 각기 접근하던 시스템 접근을 '시스템 접근제어'와 'DB 접근제어'등을 통해서만 접근하도록 하거나 통합을 확장하여 PAM 시스템 기반으로 통합 관리하기 시작한다. 또한 '식별자·신원' 영역에서는 Directory, 그룹웨어, IAM 등을 연계하여 사용자 계정과 권한 신청 프로세스를 통합하는 등, 각 영역별로 정책 관리의 중앙화를 추진한다.

✓ **정책 변경이 자동으로 이루어지는가?**

- 정책 변경이 '기존' 단계의 개별 수동 작업에서 벗어나, 일부 자동화된 통합 시스템에 의해 이루어진다.

실무 환경에서는 '엔드포인트' 영역의 경우, 정보보안포털이나 UEM 시스템 콘솔 등에서 정책을 수정하면 별도 관리되는 EPP, EDR, NAC, MDM 등에 정책이 자동으로 반영된다. '애플리케이션' 영역에서는 CSPM(클라우드 보안 형상 관리) 기능을 통해 여러 클라우드 환경의 보안 정책을 중앙에서 확인(통합 가시성)하는 등, 초기 수준의 자동화가 구현된다. 다만, 모든 시스템에 대한 완전한 동적 자동화(예시: SOAR 연동)는 구현되지 않아, 연동되지 않은 레거시 시스템이나 복잡한 환경에서는 여전히 수동 조정이 필요하다.

■ **향상**

✓ **실시간 보안 이벤트를 기반으로 정책을 동적으로 조정하는가?**

- SIEM/SOAR, EDR, UEBA, ZTNA 등에서 탐지된 실시간 보안 이벤트를 트리거(Trigger)로 사용하여 정책이 동적으로 조정되는 연계 체계가 구축된 상태이다. 실무 환경에서는 탐지된 위협 정보가 정책 결정지점(PDP)(예시: ICAM, ZTNA 컨트롤러)으로 전달되어, 리스크 스코어링 및 정책 재조정이 이루어진다.

✓ **위협에 따라 즉각적으로 정책을 수정하고 적용하는 자동화된 프로세스가 존재하는가?**

- 정책결정지점(PDP)에서 결정된 동적 정책(예시: 특정 사용자 접근 차단)은 SOAR의 플레이북이나 API 연동을 통해 정책시행지점(PEP)(예시: NGFW, PAM, 마이크로 세그멘테이션)에 즉각적으로 수정 및 적용된다. 또한, 정책 변경 전후에 대한 검증 및 롤백(Rollback)을 위한 복구 프로세스도 자동화되어 위협 대응의 일관성과 안정성을 확보한다.

■ **최적화**

✓ **AI 기반의 자율 정책 통합 시스템을 통해, 상황에 맞게 정책을 자동으로 조정 가능한가?**

- ML/AI 기반의 자율 정책 통합 시스템이 구축되어, 모든 보안 정책이 중앙에서 자동으로 관리되고 최적화되는 단계이다. 실무 환경에서는 개별 시스템이나 빅데이터 플랫폼에 적용되어 있는 AI 엔진이 SIEM, XDR, CTI 등에서 수집된 방대한 데이터를 실시간으로 분석하여, UEBA를 기반으로 정책을 동적으로 조정한다. 나아가, 정책결정지점(PDP)(예시: ICAM, ZTNA 등)은 새로운 위협을 예측하여 사전에 정책을 최적화하며, 정책 변경이 정책시행지점(PEP)(예시: NGFW, ZTNA, CNAPP 등)에 적용되기 전, AI가 해당 변경이 미칠 영향도를 자동으로 평가(시뮬레이션)하여 잠재적인 서비스 장애나 문제 발생 가능성을 사전에 차단하는 자율적인 정책 통합관리가 이루어진다.

항목	8.2 중요 프로세스 자동화	
설명	보안 및 운영에 필요한 핵심 프로세스를 자동화하여, 업무의 효율성을 높이고 인적 오류를 줄이는 것을 목표로 한다. 이는 중요한 시스템 이벤트 처리, 데이터 백업, 장애 대응 등의 프로세스를 포함한다.	
성숙단계	기존	수동 절차에 의존하며, 핵심 보안 및 운영 프로세스가 수동으로 관리되는가?
	초기	중요한 프로세스에 대한 자동화 도구를 도입하여, 반복적인 작업과 기본적인 보안 절차를 자동으로 처리하는가?
		데이터 백업 및 기본 장애 대응과 같은 주요 업무가 자동화되어 있는가?
	향상	자동화된 프로세스를 확장하여, 보안 사고 발생 시 신속한 자동 대응이 가능한가?
	최적화	자동화 시스템은 모든 프로세스를 실시간으로 최적화하고, 업무 중단 없이 중요한 프로세스를 자동으로 조정 가능한가?

세부 설명

■ **기존**

✓ **수동 절차에 의존하며, 핵심 보안 및 운영 프로세스가 수동으로 관리되는가?**

- 모든 핵심 보안 및 운영 프로세스(데이터 백업, 장애 대응, 보안 이벤트 처리 등)가 SOAR와 같은 자동화 도구 없이 수동으로 관리되는 단계이다. 실무 환경에서는 프로세스 실행 절차가 엑셀, 워드 등 문서 기반(예시: 장애 대응 매뉴얼)으로 관리되며, 각 시스템에서도 경보(Alert)가 발생하더라도, 담당자가 이를 인지한 후 관련 정책시행지점(PEP)(예시: 방화벽, EPP, PAM 등)에 직접 접속하여 수동으로 정책을 적용한다.

■ **초기**

✓ **중요한 프로세스에 대한 자동화 도구를 도입하여, 반복적인 작업과 기본적인 보안 절차를 자동으로 처리하는가?**

- 초기 수준의 자동화 도구를 통해 반복적인 작업과 기본적인 보안 절차를 자동으로 처리하기 시작한다. 실무 환경에서는 SIEM을 통한 이벤트 수집이나 EPP/PMS를 통한 패치 배포가 자동화된다. 또한, SIEM에서 탐지된 기본적인 위협(예시: 알려진 악성 IP 접근)에 대해, SOAR의 간단한 플레이북을 통해 NGFW(예시: 해당 IP 차단 규칙) 시스템 등에 기본 정책이 자동으로 추가되는 수준을 의미한다.

✓ **데이터 백업 및 기본 장애 대응과 같은 주요 업무가 자동화되어 있는가?**

- 정해진 시간에 데이터 백업 스크립트가 자동으로 실행되거나, 서비스 장애 감지 시 자동 재시작 스크립트가 실행되는 등 주요 운영 업무가 자동화된다. 실무 환경에서는 RPA(로보틱 프로세스 자동화)와 같은 도구를 활용하여, '주기적인 백업 프로세스 자동화'나 '방화벽 정책 신청 시 자동 반영' 등 반복적이면서 중요한 IT 운영 프로세스를 자동화하는 것도 이 단계에 포함될 수 있다.

■ **향상**

✓ **자동화된 프로세스를 확장하여, 보안 사고 발생 시 신속한 자동 대응이 가능한가?**

- SOAR 시스템이 SIEM, XDR UEBA 등과 연동되어, 보안 사고 발생 시 신속한 자동 대응이 가능한 연계 체계가 구축된 상태이다. 실무 환경에서는 랜섬웨어 감염 징후, 비정상적인 내부망 접속 등 단순 규칙을 넘어서는 복합 위협이 SIEM이나 XDR을 통해 탐지될 경우, 즉시 SOAR가 트리거된다. SOAR는 사전에 정의된 플레이북(Playbook)에 따라, 정책시행지점(PEP)(예시: ZTNA, 마이크로 세그멘테이션, CNAPP 등)과 연동하여 '의심 파일 실행 제한', '감염된 기기의 네트워크 격리', '관련 계정 일시 잠금' 등 실시간 위협 대응을 자동화한다. 이 모든 대응 이력은 정보보안 포털이나 SOAR 대시보드를 통해 중앙에서 관리되어 수동 개입을 최소화하고 대응 시간(MTTR)을 단축시킨다.

■ **최적화**

✓ **자동화 시스템은 모든 프로세스를 실시간으로 최적화하고, 업무 중단 없이 중요한 프로세스를 자동으로 조정 가능한가?**

- '향상' 단계의 신속한 자동 대응이 확장되어, 위협을 사전에 평가하고 시스템 취약점 패치까지 완료하는 완전한 자율 운영 단계이다. ML/AI 기반의 자율 운영 체계가 구축되어, 모든 프로세스를 실시간으로 최적화하고 업무 중단 없이 동적으로 조정한다. 실무 환경에서는 AI 엔진이 트래픽 패턴, 위험 지표, 사용자 행동(UEBA)을 실시간으로 분석하여, 정책결정지점(PDP)(예시: ICAM)의 동적 리스크 스코어링을 최적화한다. 또한, 보안 위협 대응뿐만 아니라, RPA 시스템과 연계되어 '신규 계정 생성 및 권한 부여', '방화벽 정책 신청/검증' 등 반복적인 IT 운영 및 보안 프로세스까지 자율적으로 처리한다. 시스템 업데이트나 새로운 보안 정책 변경 시, AI가 다양한 시나리오 시뮬레이션을 통해 잠재적 영향도(예시: 업무 중단 가능성)를 사전에 평가하고, 검증이 완료된 정책만 정보보안 포털 승인 워크플로우를 거쳐 SOAR를 통해 무중단으로 배포/전환하는 등, 보안성과 운영 효율성을 모두 달성하는 자율적인 체계를 의미한다.

항목	8.3 인공지능	
설명	보안 위협을 감지하고 분석하는데 있어 인간의 개입을 최소화하고, 네트워크와 시스템에서 발생하는 데이터를 기반으로 보안 결정을 자동화하는 기능을 제공한다.	
성숙단계	기존	데이터를 수동으로 수집하고 분석하며, 보안 위협에 대한 대응도 수동으로 이루어지는가?
	초기	기본적인 AI 기반 도구를 도입하여 보안 이벤트를 분석하고 패턴을 식별하는가?
	향상	AI 기반의 보안 시스템이 고도화되어, 실시간으로 위협을 탐지하고 대응 가능한가?
	최적화	AI가 모든 보안 시스템에 완전히 통합되었는가?
		자율적으로 보안 위협을 감지하고 대응하며, 정책을 동적으로 조정 가능한가?

세부 설명

■ **기존**

✓ **데이터를 수동으로 수집하고 분석하며, 보안 위협에 대한 대응도 수동으로 이루어지는가?**

- AI(인공지능) 기술이 적용되지 않은 상태로, 보안 로그, 네트워크 트래픽, 시스템 이벤트 등 모든 데이터를 수동으로 수집·분석하는 단계이다. 실무 환경에서는 SIEM이나 UEBA 시스템과 같은 자동화된 분석 도구가 부재하고, 각 시스템에서 개별적으로 추출된 문서 기반 데이터(엑셀, 워드 등)를 분석하며, 보안 담당자가 직접 패턴 분석, 이상 징후 식별, 위협 판단을 수행하고, 보안 위협에 대한 대응(예시: 정책시행지점(PEP) 정책 변경)도 수동으로 이루어지는 상태이다.

■ **초기**

✓ **기본적인 AI 기반 도구를 도입하여 보안 이벤트를 분석하고 패턴을 식별하는가?**

- ML/AI 기반 AI 도구를 도입해 보안 이벤트 자동 분석을 시작한 단계이다. 실무 환경에서는 NGFW, EPP, SIEM 등에 내장된 기본적인 머신러닝(지도 학습) 기능을 활용하여, 알려진 공격 시그니처(예시: 악성 IP, C&C 패턴)를 식별하거나 스팸 메일, 기본 랜섬웨어 등 반복적인 위협을 탐지한다. 이 단계는 UEBA와 같은 고도화된 비지도 학습이나 행동 분석보다는, 시그니처 기반 탐지를 보조하는 수준의 초기 AI 적용 단계에 해당한다.

■ **향상**

✓ **AI 기반의 보안 시스템이 고도화되어, 실시간으로 위협을 탐지하고 대응 가능한가?**

- ML/AI 기반의 보안 시스템이 고도화되어 실시간 분석 및 자동화된 대응을 수행한다. 실무 환경에서는 SIEM이나 XDR 시스템 등에 UEBA기능이 통합되거나 전용 UEBA 시스템이 연동된다. 이를 통해 스트리밍 데이터(실시간 로그)를 기반으로 사용자와 기기의 행동을 심층 분석하고, 알려지지 않은 위협(비정상 행위)을 실시간으로 탐지한다. 탐지된 위협은 SOAR, ICAM 시스템 등에 연동되어 자동화된 대응(예시: 티켓 생성, 관리자 알림, 정책시행지점(PEP) 차단)을 수행하기 시작한다.

■ **최적화**

✓ **AI가 모든 보안 시스템에 완전히 통합되었는가?**

- AI가 단순한 분석 도구를 넘어, 전사 보안 시스템을 능동적으로 조율하는 Agentic AI(에이전트형 AI) 형태로 통합된 상태이다. 실무 환경에서는 AI 엔진이 중앙의 보안 에이전트로서 각 보안 시스템(SIEM, EDR, ZTNA, CNAPP 등)을 통합하여 관리할 수 있다. 분산된 보안 데이터를 단일 관점에서 분석하는 것을 넘어, AI가 스스로 판단하여 필요한 시스템에 명령을 내리고 결과를 회신받아 다음 행동을 결정하는 유기적인 통합 아키텍처가 구성된다.

✓ **자율적으로 보안 위협을 감지하고 대응하며, 정책을 동적으로 조정가능한가?**

- Agentic AI 기술을 적용하여 자율형 사이버 대응체계를 구축한다. 실무 환경에서는 AI 에이전트가 위협 발생 시 스스로 목표(예: 위협 격리 및 서비스 복구)를 설정하고, CTI 정보 분석, 영향도 평가, 정책 시뮬레이션, 차단 및 복구 등의 복잡한 대응 시나리오를 스스로 계획하고 실행한다. 예시로 실시간으로 사용자/기기의 동적 리스크 스코어를 산출하고, 정책결정지점(PDP)(예시: ICAM)은 이 스코어를 기반으로 '위험 점수 기반 접근제어'를 수행하며, SOAR와 연동하여 정책시행지점(PEP)의 정책을 자율적으로 조정한다. 또한, AI 시스템은 새로운 위협과 대응 결과를 지속적으로 자율 학습하여(예시: 자동화된 플레이북 개선), 탐지 정확도와 대응 속도를 스스로 진화시키고 보안 체계를 실시간 최적화한다.

항목	8.4 보안 통합, 자동화 및 대응	
설명	SOAR는 보안 이벤트에 대한 대응을 자동화하고, 여러 보안 도구와 시스템을 통합하여 일관된 보안 오케스트레이션을 수행하는 시스템이다. 이를 통해 조직은 보안 사고에 신속하게 대응하고, 반복적인 작업을 자동화하여 운영 효율성을 높일 수 있다.	
성숙단계	기존	보안 도구와 시스템이 각각 독립적으로 운영되며, 수동 대응에 의존하는가?
		보안 사고 발생 시 여러 도구에서 데이터를 수집하고 분석하며, 대응 절차도 개별적으로 수행되는가?
	초기	SOAR 시스템을 도입하였는가?
		보안 이벤트는 여러 시스템에서 데이터를 수집하여 중앙에서 대응 가능하도록 관리되고 있는가?
	향상	SOAR 시스템을 고도화하여 복잡한 보안 사고에 대해 자동화된 대응과 실시간 통합이 가능한가?
		여러 도구와 연동하여 신속한 위협 차단이 가능한가?
	최적화	모든 보안 이벤트가 중앙에서 자동으로 처리되는가?
		자율 통합을 통해 자동으로 보안 사건 관리가 되는가?

세부 설명

■ 기존

✓ **보안 도구와 시스템이 각각 독립적으로 운영되며, 수동 대응에 의존하는가?**

- 방화벽, EPP, SIEM 등 개별 보안 도구가 연동되지 않고 독립적으로 운영되는 단계이다. 실무 환경에서는 보안 도구 간 정보 공유가 미비하여 위협 상관관계를 분석하기 어렵고, 모든 대응이 담당자의 수동 조치에 의존하는 상태이다.

✓ **보안 사고 발생 시 여러 도구에서 데이터를 수집하고 분석하며, 대응 절차도 개별적으로 수행되는가?**

- 보안 사고 발생 시, 자동화된 플레이북(Playbook)이 없어 담당자가 각 도구별로 로그를 수동으로 취합하고 분석한다. 실무 환경에서는 SIEM 시스템에서 탐지된 경보를 바탕으로, 담당자가 다시 보안 시스템 콘솔에 접속해 악성코드 행위를 분석하고, 방화벽 관리 콘솔에 접속해 관련 IP를 차단하는 등 대응 절차가 개별 시스템에서 독립적으로 수행된다. 이로 인해 대응 시간(MTTR)이 길어지고, 인적 실수(Human Error)가 발생할 가능성이 높은 상태이다.

■ 초기

✓ **SOAR 시스템을 도입하였는가?**

- SOAR 시스템을 도입하여 SIEM, EDR 시스템 등 주요 보안 도구를 연동하고, 기본적인 자동화 워크플로우인 '플레이북(Playbook)'을 구축하기 시작한 상태이다. 실무 환경에서는 '알려진 악성 IP 탐지 시'와 같은 단순하고 반복적인 이벤트에 대해, SOAR가 자동으로 티켓을 생성하고 담당자에게 알림을 보내는 등 초기 수준의 자동화가 적용된다.

✓ **보안 이벤트는 여러 시스템에서 데이터를 수집하여 중앙에서 대응 가능하도록 관리되고 있는가?**

- SIEM, EPP, 방화벽 등 일부 시스템의 경보(Alert)가 SOAR로 연동되어 사고 정보가 중앙으로 집계되고, 대응 프로세스가 통합되기 시작한다. 실무 환경에서는 보안 사고 발생 시, 담당자가 개별 시스템에 일일이 접속하는 대신 SOAR 대시보드에서 관련 정보를 취합하고, 플레이북을 통해 대응을 시작하는 등 중앙에서 조율 가능한(Orchestration) 관리 체계가 마련된다.

■ **향상**

✓ **SOAR 시스템을 고도화하여 복잡한 보안 사고에 대해 자동화된 대응과 실시간 통합이 가능한가?**

- SOAR 시스템이 SIEM, XDR, UEBA 시스템 등 다양한 보안 도구와 API 연동을 통해 고도화되어, 복잡한 보안 사고에 대해 실시간 대응이 가능한 수준이다. 실무 환경에서는 XDR이나 UEBA가 탐지한 '복합 위협 시나리오(예시: 계정 탈취 후 내부 횡적 이동 징후)를 SOAR가 인지하며, 정교하게 구성된 대응 시나리오(플레이북)를 기반으로 자동화된 대응을 시작한다.

✓ **여러 도구와 연동하여 신속한 위협 차단이 가능한가?**

- SOAR 플레이북이 여러 도구와 연동하여 신속한 위협 차단을 수행한다. 실무 환경에서는 보안 이벤트 발생 시, SOAR가 EDR을 통해 '엔드포인트 격리'를 수행하고, ZTNA/NGFW와 연동하여 '네트워크 접근 차단'을 지시하며, ICAM 시스템과 연계하여 '의심 계정 비활성화'를 실행하는 등, 여러 정책시행지점(PEP) 및 보안 시스템과 연동된 차단/격리 조치가 자동으로 수행된다.

■ **최적화**

✓ **모든 보안 이벤트가 중앙에서 자동으로 처리되는가?**

- 모든 보안 이벤트가 중앙 SIEM/SOAR 시스템에 자동으로 수집·정규화·분석되며, 우선순위에 따라 자율적으로 대응 흐름이 실행된다. 실무 환경에서는 ML/AI 기반의 자동 의사결정 엔진(예시: SOAR 내 AI 모듈, ICAM 내 신뢰도 판단 엔진 등)이 SIEM, XDR, UEBA 시스템 등에서 수집된 공격 유형, 자산 특성, 과거 이력 등을 종합적으로 분석하여, 사람의 개입 없이도 적절한 대응 조치(플레이북)를 스스로 판단하고 실행한다.

✓ **자율 통합을 통해 자동으로 보안 사건 관리가 되는가?**

- 보안 사건 관리 전 과정(예시: 보안 이벤트 탐지, 분류, 분석, PDP의 동적 정책 결정, SOAR를 통한 PEP의 정책 실행, 복구, 리포트 발행 등)이 완전히 자동화되어, 사람의 개입이 최소화된 상태이다. 실무 환경에서는 AI가 단순 대응을 넘어, 복잡한 위협 시나리오 전체를 자율적으로 처리하고, 대응 결과를 정보보안 포털 등에 자동으로 보고하는 등, 보안 운영(SecOps) 자체가 자동화된 자율 통합 체계를 의미한다.

항목	8.5 데이터 교환 표준화	
설명	조직 내외부에서 발생하는 다양한 데이터를 일관된 형식으로 관리하고, 보안 시스템 간에 효율적으로 데이터를 공유할 수 있도록 하는 프로세스이다. 이를 통해 여러 시스템에서 수집된 데이터를 통합적으로 분석하고, 보안 위협에 대응할 수 있다.	
성숙단계	기존	수집된 데이터가 상이한 형식으로 저장되는가?
		데이터 교환이 비효율적으로 이루어지는가?
		보안 시스템 간 데이터 교환이 수동으로 이루어지는가?
	초기	데이터 교환 표준을 도입하였는가?
		보안 시스템 간 데이터 교환이 자동화되었는가?
	향상	다양한 외부 시스템 및 파트너와도 데이터 공유가 원활하게 이루어지는가?
		여러 보안 도구 간의 상호 운용성이 제공되는가?
	최적화	데이터 교환 표준화가 자율적으로 관리되며, 외부 파트너와의 데이터 교환까지 실시간으로 자동화되는가?
		모든 시스템에서 일관된 데이터 형식이 적용되어 있는가?
		보안 위협이 발생할 때마다 실시간으로 데이터를 교환하고 분석하는가?

세부 설명

■ 기존

✓ **수집된 데이터가 상이한 형식으로 저장되는가?**

- 수집된 데이터가 통합로그 시스템이나 SIEM 등 중앙 시스템에서 표준화되지 않고, 각 시스템별로 상이한 형식(예시: CSV, TXT, JSON, 개별 DB 테이블)으로 저장된다. 실무 환경에서는 로그 저장을 위한 정해진 템플릿이나 연동 표준이 부재하여, 시스템 간 로그를 통합하여 활용(예시: 상관관계 분석)하기 어렵다.

✓ **데이터 교환이 비효율적으로 이루어지는가?**

- 데이터 교환이 SCIM(계정 정보 교환), SAML/OAuth(인증 토큰 교환)와 같은 표준 프로토콜 기반이 아닌, 비효율적인 방식으로 이루어진다. 실무 환경에서는 필요한 데이터를 엑셀로 수동 추출하여 이메일로 전달하거나, 각 시스템 연동 시 표준 API 없이 개별 조직 환경에 맞춘 커스텀 스크립트(예시: DB 직접 조회 스크립트)를 개발하여 사용한다.

✓ **보안 시스템 간 데이터 교환이 수동으로 이루어지는가?**

- 보안 시스템 간 데이터 교환(예시: SIEM과 IAM간의 사용자 정보 연동) 시 Restful API와 같은 표준화된 연동 방식이 부재하다. 실무 환경에서는 연동을 위해 각 시스템 환경에 맞춘 커스텀 에이전트(Agent)를 별도로 컴파일하여 설치하거나, 담당자가 스크립트를 수동으로 실행하여 데이터를 전송하는 등 자동화되지 않은 방식으로 운영된다.

■ **초기**

✓ **데이터 교환 표준을 도입하였는가?**

- 표준 프로토콜을 도입하기 시작하는 단계이다. 실무 환경에서는 예시로 SAML, , OIDC, OAuth 등 표준 프로토콜을 사용하여 SSO(통합인증)나 IAM(통합계정권한관리) 시스템 간의 인증 정보 교환을 표준화하거나, Restful API를 활용하여 데이터 교환을 시도한다. 또한 SCIM 표준 프로토콜과 같은 계정 프로비저닝 표준이 일부 시스템에 적용되기 시작한다.

✓ **보안 시스템 간 데이터 교환이 자동화되었는가?**

- 보안 시스템 간 데이터 교환이 SOAR 시스템 등을 통한 실시간 연동이 아닌, 정기적인 배치(Batch)나 예약된 스케줄 기반으로 자동화된다. 실무 환경에서는 ETL(Extract, Transform, Load) 도구나 스케줄링된 스크립트가 Restful API를 호출하여 SIEM의 로그를 빅데이터 플랫폼으로 전송하거나, IAM의 계정 정보를 PAM 시스템으로 주기적으로 DB 동기화하는 등의 비실시간 자동화 방식이 주로 사용된다.

■ **향상**

✓ **다양한 외부 시스템 및 파트너와도 데이터 공유가 원활하게 이루어지는가?**

- 데이터 교환이 조직 내 주요 시스템은 물론 외부 파트너 시스템까지 확장되며 상호 운용성과 실시간성이 높아지는 단계이다. 실무 환경에서는 외부 CTI 피드나 클라우드 보안 정보 수신 시, 해당 데이터를 수집 단계에서부터 정제화(Refinement)하고, 통합로그 시스템이나 SIEM, 빅데이터 플랫폼 등 내부 시스템과 연동할 수 있도록 정의된 로그 포맷(예시: CEF, LEEF)이나 DB 테이블 스키마에 맞춰 변환(Formatting)하여 통합 관리한다.

✓ **여러 보안 도구 간의 상호 운용성이 제공되는가?**

- SAML, SCIM, Restful API 등 표준화된 데이터 교환 체계가 전사적으로 도입되어, 여러 보안 도구 간의 상호 운용성이 확보된다. 실무 환경에서는 SIEM, XDR, SOAR, ICAM 등 개별 보안 시스템이 단방향 경보(Alert) 전송을 넘어, 표준화된 형식(예시: JSON API)을 통해 데이터를 상호 교환(연동)한다. 이를 통해 통합로그 시스템이나 SIEM, 빅데이터 플랫폼 같은 중앙 분석 시스템이 이기종 시스템의 데이터를 바탕으로 고도화된 상관관계 분석을 수행할 수 있는 기반이 마련된다.

■ **최적화**

✓ **데이터 교환 표준화가 자율적으로 관리되며, 외부 파트너와의 데이터 교환까지 실시간으로 자동화되는가?**

- 데이터 교환 표준(예시: SCIM, SAML, STIX/TAXII)과 메타데이터 정책이 ML/AI 기반으로 자율적으로 관리된다. 실무 환경에서는 시스템이 데이터 교환 표준의 준수 여부를 자동으로 검증·모니터링하며, 오류 발생 시(예시: 비표준 API 호출, 스키마 불일치) SOAR와 연동하여 자율적으로 복구하거나(예시: 임시 롤백) 관리자에게 즉각 알림을 보낸다. 또한, 내부 시스템 간 데이터 교환뿐 아니라 외부 파트너(공공기관, 협력사 등)와의 연동도 Restful API 게이트웨이 등을 통해 실시간으로 처리되는 자율 운영 체계가 구축된다.

✓ **모든 시스템에서 일관된 데이터 형식이 적용되어 있는가?**

- 전사 보안 시스템은 물론 모든 IT 시스템(예시: HRM, ERP)에서 동일한 데이터 구조 및 스키마(예시: 공통 데이터 모델, CEF/LEEF)가 적용된다. 실무 환경에서는 빅데이터 플랫폼이나 SIEM에 저장된

데이터가 별도의 포맷 변경(파싱, 정규화) 과정 없이, 모든 연동 시스템(SOAR, UEBA, ICAM 등)에서 일관된 데이터 형식으로 즉시 처리가 가능하다.

✓ **보안 위협이 발생할 때마다 실시간으로 데이터를 교환하고 분석하는가?**

- 보안 위협이 발생할 때마다, 실시간으로 관련 이벤트 및 대응 데이터가 표준화된 AP를 통해 자동으로 수집·분석·공유된다. 실무 환경에서는 XDR이 위협을 탐지하면, 해당 위협 정보가 즉시 SOAR와 CTI 플랫폼으로 공유된다. SOAR는 이 정보를 바탕으로 정책결정지점(PDP)(예시: ICAM)에 리스크 스코어링을 요청하며, PDP는 다시 정책시행지점(PEP)(예시: SSO, PAM, ZTNA, 마이크로 세그멘테이션 등)에 동적 정책을 전달하는 등, 모든 보안 시스템이 표준화된 데이터를 기반으로 실시간 상호작용(데이터 교환 및 분석)을 수행한다.

항목	8.6 보안 운영 조정 및 사고 대응	
설명	조직 내 보안 사고가 발생했을 때, 이를 신속하게 대응하고 조직 내 여러 부서와 조율하여 보안 문제를 해결하는 프로세스를 의미한다. 이를 통해 보안 사고가 발생할 때 적절한 대응 절차를 신속하게 이행할 수 있으며, 피해를 최소화할 수 있다.	
성숙단계	기존	보안 팀이 수동으로 여러 부서와 소통하고 조정하는가?
		보안 사고 대응 절차가 정형화되어 있지 않는가?
	초기	보안 사고 대응 계획을 수립하고, 사고 대응 절차를 표준화하였는가?
		보안 사고가 발생하면 자동화된 경고가 생성되는가?
	향상	사고 대응 절차가 자동화되고, 보안 운영팀과 다른 부서 간 조율이 실시간으로 이루어지는가?
		자동화된 보고 시스템을 통해 보안 사고의 진행 상황이 지속적으로 공유되는가?
	최적화	보안 사고가 발생하기 전에 이를 예측하고 선제적으로 대응 가능한가?
		사고 대응 절차는 완전히 자동화되어, 보안 팀과 관련 부서가 신속하고 일관된 대응이 가능한가?
		사고 발생 시 모든 관련 부서가 실시간으로 협력하고, 대응 결과가 즉시 보고되는가?

세부 설명

■ **기존**

✓ **보안 팀이 수동으로 여러 부서와 소통하고 조정하는가?**

- 보안 사고 발생 시, 보안 팀이 개별 부서(예시: IT 인프라팀, 현업 부서)와 전화, 이메일, 메신저 등을 통해 직접 연락하고 협의하여 대응하는 단계이다. 정보보안 포털 같은 자동화된 협업 도구가 부재하여, R&R(역할 및 책임)에 따른 명확한 협업 절차가 정립되어 있지 않다.

✓ **보안 사고 대응 절차가 정형화되어 있지 않는가?**

- 보안 사고에 대한 대응 및 운영 조정이 주로 수동 절차에 의존하며 체계화되지 않은 상태이다. 실무 환경에서는 문서화된 표준운영절차(SOP)나 사고 대응 흐름도가 부재하여, 담당자의 경험에 의존하는 사건별 임기응변식 대응이 일반적이다. 이로 인해 대응 품질이 일관되지 않고 누락이 발생할 수 있다.

■ **초기**

✓ **보안 사고 대응 계획을 수립하고, 사고 대응 절차를 표준화하였는가?**

- 보안 사고 대응 계획 및 절차가 수립되며, 자동화된 경보(개별 시스템 Alert, SIEM 등) 기반의 초기 대응 체계가 마련되는 단계이다. 실무 환경에서는 보안 사고 대응 체계를 구성하고, 위협 유형별(예시: 악성코드 감염, 계정 탈취 시도) 정형화된 대응 프로세스 및 시나리오를 SOP(표준운영절차)로 문서화하여 관리하기 시작한다.

✓ **보안 사고가 발생하면 자동화된 경고가 생성되는가?**

- 개별 보안 솔루션이나 SIEM을 통해, 사전에 정의된 정적 규칙(Static Rule)에 기반하여 자동화된 경고(Alert)가 생성되고, 일정 조건 하에 담당자(예시: SOC(보안 운영 센터) 1차 관제)에게 전달된다. 실무 환경에서는 사고 발생 시 대응 책임자(보안팀)와 협업 부서(IT팀)가 명확히 지정되어 있으며, SOAR 시스템과 같은 자동화된 협업 도구는 없지만 정의된 R&R(역할 및 책임)에 따라 이메일, 전화 등으로 연락하는 기초적인 역할분담 체계가 운영된다.

■ **향상**

✓ **사고 대응 절차가 자동화되고, 보안 운영 팀과 다른 부서 간 조율이 실시간으로 이루어지는가?**

- 보안 운영 및 사고 대응 절차가 SOAR의 플레이북을 통해 자동화되고, 부서 간 협업 체계가 실시간으로 작동하는 단계이다. 실무 환경에서는 SIEM이나 XDR 등에서 분석된 위협이 SOAR로 전달되면, 사전에 정의된 R&R(역할 및 책임)에 따라 자동화된 워크플로우가 실행된다. (예시: SOAR가 IT지원팀에는 '기기 격리' 티켓을, 법무/인사팀에는 '내부자 위협 알림'을, 정보보안 포털에는 '진행 상황'을 동시에 자동 전송) 또한, Slack, Teams 등 통합 커뮤니케이션 도구와 연동되어 관련 부서 간 실시간 조율 체계가 마련된다.

✓ **자동화된 보고 시스템을 통해 보안 사고의 진행 상황이 지속적으로 공유되는가?**

- 자동화된 보고 시스템을 통해 사고 처리 진행 상황과 결과가 전사적으로 공유된다. 실무 환경에서는 SOAR의 케이스 관리 기능이나 정보보안 포털이 중앙 대시보드 역할을 수행한다. 위협 탐지(예시: SIEM 경보)부터 대응 완료(예시: SOAR 플레이북 완료)까지의 모든 진행 상황이 이 대시보드에 실시간으로 업데이트되며, 경영진 및 관련 부서가 현재 보안 태세와 사고 대응 현황을 지속적으로 공유받을 수 있는 체계가 마련된다.

■ **최적화**

✓ **보안 사고가 발생하기 전에 이를 예측하고 선제적으로 대응 가능한가?**

- ML/AI 기반의 예측 분석 시스템이 구축되어, SIEM, XDR, CTI 피드, UEBA 로그 등 방대한 데이터를 실시간으로 분석하여 잠재적 위협을 조기에 예측하고 선제적으로 대응 가능한 수준이다. 실무 환경에서는 AI 엔진이 과거 공격 데이터와 실시간 CTI 정보, 내부 사용자/기기의 행동 패턴을 지속적으로 학습하여, 단순 이상 징후를 넘어 '제로데이 공격 징후'나 '내부자 위협(예시: 퇴사 예정자의 비정상적 데이터 접근 패턴)'을 사전에 예측한다. 이 예측 정보는 정책결정지점(PDP)(예시: ICAM)의 동적 리스크 스코어링에 즉각 반영되어, 위협이 실제 발생하기 전에 선제적인 대응(예시: 고위험 계정의 권한 자동 축소, 의심 기기의 모니터링 강화)을 수행한다.

✓ **사고 대응 절차는 완전히 자동화되어, 보안 팀과 관련 부서가 신속하고 일관된 대응이 가능한가?**

- 사고 대응 절차는 AI와 SOAR의 플레이북 등을 통해 정책 기반으로 자동 실행되며, 일련의 대응 프로세스가 담당자의 수동 개입 없이 동작 가능하다. 실무 환경에서는 AI가 위협(예시: 랜섬웨어 확산 징후)을 탐지하고 위험도를 판단하면, SOAR가 고도화된 플레이북을 자율적으로 실행한다. 이 플레이북은 정책결정지점(PDP)(예시: ICAM)의 정책 결정을 받아, 정책시행지점(PEP)(예시: ZTNA, 마이크로 세그멘테이션, CNAPP 등)과 연동하여 '관련 워크로드 즉시 격리', '악성코드 유포 계정 비활성화', 'C&C 서버 통신 차단' 등 신속하고 일관된 대응을 자동으로 수행한다.

✓ **사고 발생 시 모든 관련 부서가 실시간으로 협력하고, 대응 결과가 즉시 보고되는가?**

- 시스템이 자동화된 대응과 동시에 실시간 협업 및 보고를 수행한다. 실무 환경에서는 사고 발생 시 SOAR 플레이북이 R&R(역할 및 책임)에 따라 보안 운영팀, 인프라팀, 서비스팀(현업), 경영진 등 모든 관련 부서에 상황을 자동으로 전파한다(예시: Slack/Teams 알림, 이메일 보고). 또한, SOAR가 정책시행지점(PEP)을 통해 수행한 모든 대응 결과(예시: '서버 3대 격리 완료', '계정 2개 잠금')는 정보보안 포털이나 중앙 대시보드에 즉시 자동으로 보고(리포팅)되어, 모든 관련 부서가 실시간으로 상황을 공유하고 협력하여 공동 대응하는 체계가 완성된다.

부록

1. 핵심 요소별 기술 및 주요 솔루션 예시

2. 핵심 요소별 증적 자료 예시

3. 용어 정의

4. 약어 정의

1. 핵심 요소별 기술 및 주요 솔루션 예시

구분	기술 및 솔루션	설명	관련 체크리스트
식별자·신원	IAM (Identity and Access Management, 통합계정권한관리)	• 사용자의 아이덴티티를 중앙에서 통제 및 관리하는 시스템 • 계정 및 권한을 통합적으로 관리하며, RBAC과 ABAC 정책 적용	1.1.1 사용자 인벤토리 1.1.2 ID 연계 및 사용자 자격 증명 1.4.1 조건부 사용자 접근
	ICAM (Identity Credential and Access Management, 통합신원계정권한관리)	• IAM에서 자격 증명(Credential) 관리가 확장된 개념으로 사용자, 디바이스 등 모든 접근 주체의 신뢰도를 동적으로 평가 • 다양한 시스템 연계를 통해 제로트러스트 아키텍처의 핵심 정책 엔진 역할을 수행	1.3.1 통합 ICAM 플랫폼 1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식 1.4.2. 최소 권한 접근
	SSO (Single Sign-On, 통합인증)	• 다양한 시스템을 한 번의 인증으로 접근하도록 지원 • 인증 진행 간 사용자의 위험도를 평가하고 동적으로 엑세스 관리	1.1.2 ID 연계 및 사용자 자격 증명 1.2.2 지속 인증
	MFA (Multi-Factor Authentication, 다중인증)	• 다중 인증 요소를 활용하여 사용자 인증 강화를 지원 • 생체정보, OTP 등을 활용한 추가 인증 수단 제공 및 패스워드리스 인증	1.2.1 다중인증 1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식
	HRM (Human Resources Management, 인사관리시스템)	• 사용자의 인사 정보(입사, 퇴사, 부서 이동, 직무)를 관리하는 시스템 • Directory/IAM/ICAM 등과 연동되어 사용자 인벤토리의 실시간 기준 정보를 제공	1.1.1 사용자 인벤토리
기기 및 엔드포인트	EDR (Endpoint Detection and Response, 엔드포인트 탐지 및 대응)	• 디바이스의 위협을 실시간으로 탐지하고 대응 • 비인가 접근을 방지하고, 디바이스에 대한 신뢰성을 지속적으로 평가	2.1.1 기기 감지 및 규정 준수 2.2.1 실시간 검사를 통한 기기 권한 부여 2.4.1 엔드포인트 및 확장된 탐지·대응
	ITAM (IT Asset Management, IT자산관리시스템)	• 조직 내 모든 IT장비를 식별 및 관리 • 다른 보안 솔루션과 실시간 연동을 통해 디바이스 상태를 실시간 모니터링	2.1.1 기기 감지 및 규정 준수 2.3.1 기기 인벤토리
	UEM (Unified Endpoint Management, 통합 엔드포인트 관리)	• 모바일 기기뿐만 아니라 다양한 IoT 기기까지 통합적으로 관리 • 개인 기기와 업무용 데이터를 분리하여 BYOD 환경을 관리 가능	2.1.1 기기 감지 및 규정 준수 2.3.2 통합 엔드포인트 관리 및 모바일 기기 관리
	EPP (Endpoint Protection Platform, 엔드포인트 보호 플랫폼)	• 디바이스에 대한 통합 보안 플랫폼 • 백신, 패치관리, 개인정보보호 등 다양한 보안기능 제공	2.4.2 자산, 취약성 및 패치 관리 자동화

구분	기술 및 솔루션	설명	관련 체크리스트
네트워크	ZTNA (Zero Trust Network Access, 제로트러스트 네트워크 접근)	• SDP(소프트웨어 정의 경계) 기반의 안전한 통신구간 설정 • 최소 권한 원칙 기반 사용자와 디바이스를 평가하고, 안전한 연결 허용	3.1.3 소프트웨어 정의 네트워킹 3.5.1 네트워크 회복성
	NGFW (Next Generation Fire-Wall, 차세대 방화벽)	• 전통적인 방화벽 기능에 IPS, SSL 복호화 등 고급 보안 기능 제공 • 애플리케이션 콘텐츠 기반 정책 설정 및 세분화된 보안 관리 기능	3.2.1 위협 대응 3.3.1 트래픽 암호화
	Micro-Segmentation (마이크로 세그멘테이션)	• 네트워크를 논리적으로 세분화하여 각 세그먼트 간의 트래픽을 관리 • 민감한 자산에 대한 접근을 최소화하며, 내부 위협 확산을 방지	3.1.1 매크로 세그멘테이션 3.1.2 마이크로 세그멘테이션
	NDR (Network Detection and Response, 네트워크 탐지 및 대응)	• 풀패킷 모니터링 기반으로 네트워크 트래픽 실시간 분석과 이상징후를 탐지 • ML/AI 기반 분석으로 네트워크 이상 트래픽을 식별하고, 자동화된 조치 수행	3.2.1 위협 대응 3.4.1 데이터 흐름 매핑 3.5.1 네트워크 회복성
시스템	PAM (Privileged Access Management, 특권 접근 관리)	• 최소 권한 원칙을 적용하여 접근 필요한 서버(Linux, Window, DB등)에 대한 계정·권한을 통합하여 관리	4.1.1 접근통제 4.2.1 PAM 4.2.2 자격 증명 관리
	취약점 관리 시스템 (Vulnerability Management System)	• 시스템(서버)의 취약점을 주기적으로 스캔하고 관리하여 보안성을 강화 • 보안 상태를 실시간으로 모니터링	4.4.1 시스템 환경에 따른 정책 관리
	백업 관리 시스템 (Backup&Recovery Management System)	• 시스템의 주요 정보를 주기적으로 백업하고 복구 가능한 환경을 제공	4.4.1 시스템 환경에 따른 정책 관리
애플리케이션 및 워크로드	SASE (Secure Access Service Edge, 보안 액세스 서비스 엣지)	• 클라우드 기반으로 분산된 환경에서도 네트워크와 보안 정책을 일관되게 적용하여 워크로드를 보호	5.1.1 리소스 권한 부여 및 통합 5.2.1 지속적인 모니터링 및 진행 중인 승인 5.3.1 원격 접속
	CNAPP (Cloud Native Application Protection Platform, 클라우드 네이티브 애플리케이션 보호 플랫폼)	• 클라우드 네이티브 환경에 대한 통합 보안 플랫폼으로 동작하며 CSPM, CWPP, CIEM 기능 등을 단일 플랫폼으로 제공	5.2.1 지속적인 모니터링 및 진행 중인 승인 5.4.2 애플리케이션 인벤토리
	CASB (Cloud Access Security Broker, 클라우드 액세스 보안 브로커)	• 클라우드에 엑세스하는 환경에서 민감 데이터 보호, 사용자 활동 모니터링 등 다양한 보안 기능을 제공	5.2.1 지속적인 모니터링 및 진행 중인 승인
	WAAP (Web Application & API Protection, 웹 애플리케이션 및 API 보호)	• API 트래픽의 메타데이터를 분석하여 웹, 디도스 공격 등 대응 • 클라우드 기반으로 API 요청에 대해 인증과 권한을 관리	5.4.1 안전한 애플리케이션 배포
	SCA (Software Composition Analysis, 소프트웨어 구성 분석)	• 오픈소스 라이브러리와 구성요소의 취약점을 식별하고 관리 • 사용 중인 오픈소스의 라이선스 준수 여부 확인 및 보안 패치 적용 지원	5.4.1 안전한 애플리케이션 배포 5.5.1 안전한 소프트웨어 개발 및 통합 5.5.2 소프트웨어 위험 관리
	SAST/DAST (Static/Dynamic Application Security Testing) 정적/동적 애플리케이션 보안 테스트)	• 소스코드 단계에서 정적 분석을 통해 취약점을 탐지하고 관리 • 실행 중인 애플리케이션 대상으로 동적 분석을 통해 취약점을 탐지하고 관리	5.4.1 안전한 애플리케이션 배포 5.5.1 안전한 소프트웨어 개발 및 통합

구분	기술 및 솔루션	설명	관련 체크리스트
데이터	DSPM (Data Security Posture Management, 데이터 태세 관리)	• 조직 내 데이터를 식별하고 민감도에 따라 분류하여 관리 • 데이터의 가시성을 확보하여 일관된 보안 정책을 적용	6.1.1 데이터 카탈로그 위험 정렬 6.1.2 기업 데이터 거버넌스 6.4.1 데이터 라벨링 및 태그 지정
	RBI (Remote Browser Isolation, 원격 브라우저 격리)	• 웹 브라우저를 격리하여 악성 웹 사이트로부터 데이터를 보호하고 격리된 환경에서 데이터를 전송	6.2.1 데이터 접근제어 6.5.1. 데이터 손실방지
	eDLP (Enterprise Data Loss Prevention, 엔터프라이즈 데이터 유출 방지)	• 민감한 데이터를 식별하고 비인가 전송을 차단하여 데이터의 유출 방지	6.1.1 데이터 카탈로그 위험 정렬 6.2.1 데이터 접근제어 6.4.1 데이터 라벨링 및 태그 지정 6.5.1 데이터 손실 방지
	eDRM (Enterprise Digital Rights Management, 엔터프라이즈 디지털 권한 관리)	• 디지털 콘텐츠와 파일에 대한 권한 관리 및 보호를 제공하여 무단 복제 및 유출을 방지	6.1.2 기업 데이터 거버넌스 6.3.1 데이터 암호화 및 권한 관리 6.5.2 데이터 모니터링 및 감지
	ECM (Enterprise Content Management, 문서중앙화)	• 기업 내 모든 문서 및 컨텐츠를 개인 단말기가 아닌 중앙 서버에 저장하여 접근·공유·보관·폐기까지 일괄된 정책으로 통합관리	6.2.1 데이터 접근제어 6.3.1 데이터 암호화 및 권한 관리 6.5.2 데이터 모니터링 및 감지
가시성 및 분석	SIEM (Security Information and Event Management, 보안 정보 및 이벤트 관리)	• 사용자, 네트워크, 애플리케이션 등에서 발생하는 방대한 로그 데이터를 수집하여 보안 위협 탐지 대응	7.1 모든 관련 활동 기록 7.2 중앙집중적 보안 정보 및 이벤트 관리 7.3 보안 위협 분석 7.5 위협 인텔리전스 통합 7.6 자동화된 동적 정책
	BigData (빅데이터)	• 대규모 데이터를 처리하고 분석하여 조직의 보안 태세 강화 • 머신러닝, AI(인공지능)와 같은 기술을 활용하여 정상 활동, 비정상 활동을 구분하여 위협을 사전 탐지	7.3 보안 위협 분석 7.5 위협 인텔리전스 통합 7.6 자동화된 동적 정책
	통합로그 솔루션 (Integrated Log Management)	• 조직 내 다양한 리소스에서 생성된 로그 데이터를 중앙에서 관리 및 분석	7.2 중앙집중적 보안 정보 및 이벤트 관리 7.5 위협 인텔리전스 통합
	ASM (Attack Surface Management, 공격 표면 관리)	• 외부 공격자의 관점에서 인터넷에 노출된 조직의 IT 자산을 식별 및 분석하여 잠재적인 위협과 취약점을 모니터링 및 분석	7.3 보안 위협 분석
	UEBA (User and Entity Behavior Analytics, 사용자 및 개체 행동 분석)	• ML/AI을 기반으로 사용자 및 개체(기기, 서버 등)의 정상 행동을 학습하고 분석하여 리스크 스코어링 근거로 제공	7.1 모든 관련 활동 기록 7.3 보안 위협 분석 7.4 사용자 및 기기 동작 분석 7.6 자동화된 동적 정책

구분	기술 및 솔루션	설명	관련 체크리스트
자동화 및 통합	SOAR (Security Orchestration, Automation and Response, 보안 오케스트레이션, 자동화 및 대응)	• 다양한 보안 도구와 데이터를 연계하여 위협 탐지 및 자동화 대응 • 보안 운영을 효율화하고 일괄된 대응 절차를 구현	8.1 정책 통합 8.2 중요 프로세스 자동화 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화 8.6 보안 운영 조정 및 사고 대응
	ML (Machine-Learning, 머신러닝)	• 대규모 데이터 패턴을 식별하고, 비정상적인 활동 탐지 • 시스템에서 수집된 데이터를 전달하고, 통합적으로 분석하여 위협 탐지 및 대응	8.2 중요 프로세스 자동화 8.3 인공지능 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화 8.6 보안 운영 조정 및 사고 대응
	AI (Artificial Intelligence, 인공지능)	• 데이터를 학습하고 분석하여 운영 절차 자동화 및 최적화 관리 • 로그 분석, 위협 탐지 대응	8.1 정책 통합 8.2 중요 프로세스 자동화 8.3 인공지능 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화 8.6 보안 운영 조정 및 사고 대응
	RPA (Robotic Process Automation, 로보틱 프로세스 자동화)	• 단순하고 반복적인 작업을 자동화 처리하여 효율성을 높이고, 인적 오류를 줄이며, 조직의 생산성을 강화	8.1 정책 통합 8.2 중요 프로세스 자동화 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화
	XDR (eXtended Detection and Response, 확장된 탐지 및 대응)	• 다양한 실시간 탐지·대응 시스템을 통합하여 엔드포인트, 네트워크, 서버, 클라우드 등 조직 전체의 위협을 하나의 플랫폼으로 통합하고 자동화된 대응체계를 제공	8.1 정책 통합 8.2 중요 프로세스 자동화 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화 8.6 보안 운영 조정 및 사고 대응

2. 핵심 요소별 증적 자료 예시

2.1 핵심 요소별 공통 증적 자료 예시

구분	핵심 요소	관련 증적 자료
공통	식별자·신원	• 사용자 계정 관리 지침 • 통합 인증 및 자격증명 관리 지침 • 인증 및 세션 관리 지침 • 통합 식별·접근 관리 정책 및 지침 • 인증 수단 및 이상행위(컨텍스트) 탐지 관리 지침 • RBAC/ABAC 관련 내부 정책/지침 • 접근권한 관리 지침
	기기 및 엔드포인트	• 기기 및 엔드포인트 보안 관리 지침 • 기기 보안 검사 및 접근통제 지침 • IT 자산 관리 지침 • 엔드포인트 및 모바일 기기 관리 지침 • 엔드포인트 위협 탐지 및 대응 지침 • 자산 및 취약점 관리 지침
	네트워크	• 네트워크 분리 및 접근통제 지침 • 마이크로 세그멘테이션 운영 지침 (애플리케이션/워크로드 단위 분리 기준 정의) • 소프트웨어 정의 네트워크 운영 지침 • 위협 탐지 및 대응 지침 • 암호화 통제 및 키 관리 지침 • 데이터 흐름 분석 및 관리 지침 • 재해복구(DR) 및 업무연속성(BCP) 관리 지침
	시스템	• 시스템 접근통제 정책 및 지침 • 특권 계정 및 접근통제 관리 지침 • 자격 증명 및 인증 관리 지침 (패스워드 작성 규칙, 갱신 주기 등) • 네트워크 분리 및 접근통제 지침 • 시스템 보안 관리 지침 (온프레미스 및 클라우드 환경별 보안 정책 포함)
	애플리케이션 및 워크로드	• 애플리케이션 및 리소스 접근통제 지침 • 보안 모니터링 및 운영 지침 • 원격 접속 보안 관리 지침 (인가 절차, 접근 단말 보안 기준 등) • 소프트웨어 개발 보안 가이드 및 운영 지침 • 애플리케이션 자산 관리 지침 • 소프트웨어 개발 보안 지침 (시큐어코딩 표준 및 SDLC 단계별 보안 절차) • 소프트웨어 위험 관리 지침 및 계획서 (위험 식별/평가/조치)
	데이터	• 데이터 분류 및 위험 평가 지침 • 데이터 거버넌스 정책 및 관리 지침 (데이터 관리 원칙 포함) • 데이터 접근제어 정책 및 지침 • 데이터 암호화 및 키 관리 지침 • 데이터 분류 및 라벨링 관리 지침 (등급별 라벨링 기준 및 태깅 규칙) • 데이터 유출 방지(DLP) 정책 및 지침 • 데이터 모니터링 및 이상행위 탐지 절차 및 지침

구분	핵심 요소	관련 증적 자료
공통	가시성 및 분석	• 로그 및 이벤트 관리 지침 (수집 대상, 보존 기간, 무결성 확보 등) • 보안 관제 및 사고 대응 지침 • 보안 위협 및 취약점 관리 지침 • 사용자 이상행위 탐지 및 대응 관리 지침 • 위협 인텔리전스 관리 지침 • 동적 보안 정책 관리 및 운영 지침
	자동화 및 통합	• 정보보호 정책·지침·절차서 (제·개정 내역 포함) • 주요 프로세스 자동화 관리 지침·절차서 • AI 기반 보안 운영 및 자동화 관리 지침 • 보안 통합 및 자동화 대응 운영 지침 • 데이터 교환 표준화 정책 및 지침 (데이터 포맷, 연동 프로토콜 표준 정의) • 보안사고 대응 정책 및 표준운영절차(SOP)

2.2 핵심 요소별 관련 증적 자료 예시

구분	기능	세부역량	관련 증적 자료
식별자·신원	1.1 식별자 관리	1.1.1 사용자 인벤토리	• 사용자 계정 관리 지침 • 사용자 계정 목록(관리대장) • 식별자 관리 시스템(Directory/HRM/IAM 등) 운영 화면 • 계정 생명주기(생성·변경·삭제) 관리 이력 • 사용자 계정 현황 정기 점검 내역
		1.1.2 ID 연계 및 사용자 자격 증명	• 통합 인증 및 자격 증명 관리 지침 • ID 관리 시스템 연동 현황 및 구성도 • 통합 인증 시스템(SSO/IAM 등) 운영 화면 • 사용자 인증 이력 및 로그 • 사용자 자격 증명 감사 내역
	1.2 인증	1.2.1 다중인증(MFA)	• 사용자 인증 및 MFA 관리 지침 • MFA 시스템 연동 현황 및 구성도 • MFA 시스템 운영 현황 및 설정 화면 • MFA 인증 이력 및 실패 로그 • 비정상 로그인 탐지 및 대응 내역
		1.2.2 지속인증	• 인증 및 세션 관리 지침 • 인증 시스템(SSO/IAM/ICAM) 정책 설정 내역 • 실시간 세션 모니터링 및 접속 로그 • 이상행위 탐지 및 추가 인증(재인증) 이력 • 세션 및 접속 상태 관리 대시보드
	1.3 위험도 평가	1.3.1 통합 ICAM 플랫폼	• 통합 식별·접근 관리 정책 및 지침 • ICAM 시스템 연동 구성도 및 현황 • ICAM 시스템 운영 화면(대시보드, 정책 설정) • 계정 및 권한 생명주기 관리 이력(자동화 로그) • 위험 기반 접근통제 및 대응 내역 • 권한 및 정책 정기 점검 보고서
		1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식	• 인증 수단 및 이상행위(컨텍스트) 탐지 관리 지침 • 생체인증 및 다중인증(MFA) 운영 설정 및 이력 • 사용자 행위(UEBA) 및 컨텍스트 분석 탐지 로그 • 컨텍스트 기반 권한 조정 및 대응 내역 • 비정상 접근 탐지 및 조치 결과 보고서
	1.4 접근관리	1.4.1 조건부 사용자 접근	• RBAC/ABAC 관련 내부 정책/지침 • 조건부 접근통제 지침 (위치, 시간, 기기 상태 등 접근 허용 기준 정의) • 조건부 접근제어 시스템(IAM/ZTNA/PAM 등) 운영 화면 • 비정상 접속 탐지 및 대응 내역(이상행위, 정책 위반 알림 및 조치 로그) • 접근 정책 유효성 검토 및 개선 내역
		1.4.2 최소 권한 접근	• 접근권한 관리 지침 • 직무별 접근권한 정의서(RBAC 매트릭스) • 권한 신청 및 변경 승인 내역(관리 시스템 워크플로우) • 권한 상승(JIT) 및 자동 회수 이력 • 접근권한 정기 검토 및 조치 결과 보고서

구분	기능	세부역량	증적 자료
기기 및 엔드포인트	2.1 정책 준수 모니터링	2.1.1 기기 감지 및 규정 준수	• 기기 및 엔드포인트 보안 관리 지침 • IT 자산(기기) 관리대장 • 단말 규정 준수 관리 시스템(EPP/NAC/EDR 등) 운영 화면 • 비준수 기기 탐지 및 조치 이력 • 단말 보안 점검 및 조치 결과 보고서(백신, 패치, 보안 설정 준수율 등)
	2.2 데이터 접근제어	2.2.1 실시간 검사를 통한 기기 권한 부여	• 기기 보안 검사 및 접근통제 지침 • 자산 접근 기기 현황 및 검사 내역 • 기기 접근 제어 시스템(NAC/EDR/ZTNA 등) 운영 화면 • 보안 미준수 기기 접근 차단 및 제어 이력 • 기기 보안 상태 정기 점검 결과 보고서
	2.3 자산관리	2.3.1 기기 인벤토리	• IT 자산관리 지침 • IT 자산(기기) 관리대장 • 관리용 단말기 지정 및 관리 현황 • 자산관리 시스템(ITAM 등) 운영 화면 • 비인가 기기 탐지 및 차단 이력 • 정기 자산 실사 보고서
		2.3.2 통합 엔드포인트 관리 및 모바일 기기 관리	• 엔드포인트 및 모바일 기기 관리 지침 • 통합 단말기 관리대장 • 통합 엔드포인트 관리 시스템(MDM/UEM 등) 운영 화면 • 보안 패치 및 정책 배포 이력 • 단말기 이상행위 탐지 및 조치 내역
	2.4 기기 위협 보호	2.4.1 엔드포인트 및 확장된 탐지·대응 (EDR 및 XDR)	• 엔드포인트 위협 탐지 및 대응 지침 • EDR/XDR 시스템 운영 화면 • 위협 탐지 및 자동 차단·격리 이력 • 위협 인텔리전스(CTI) 연동 및 정책 반영 내역 • 위협 분석 및 대응 결과 보고서
		2.4.2 자산, 취약성 및 패치 관리 자동화	• 자산 및 취약점 관리 지침 • 취약점 및 패치 관리 시스템(EPP/EDR/PMS 등) 운영 화면 • 자산별 취약점 현황 목록 • 보안 패치 자동 배포 및 적용 내역 • 취약점 점검 및 조치 결과 보고서
네트워크	3.1 네트워크 세분화	3.1.1 매크로 세그멘테이션	• 네트워크 구성도 (전체/영역별) • 네트워크 분리 및 접근통제 지침 • 네트워크 접근제어 정책(ACL/VLAN 등) 설정 내역 • 세그먼트 간 트래픽 모니터링 및 차단 로그 • 주요 네트워크 장비(방화벽 등) 정책 검토 내역
		3.1.2 마이크로 세그멘테이션	• 마이크로 세그멘테이션 운영 지침(애플리케이션/워크로드 단위 분리 기준 정의) • 애플리케이션/워크로드 단위 상세 네트워크 구성도 • 주요 워크로드 트래픽 흐름도(Flowchart) 및 연동 구성도 • 마이크로 세그멘테이션 시스템(SDN/호스트방화벽) 설정 내역 • 세그먼트별 비인가 트래픽 차단 및 제어 로그
		3.1.3 소프트웨어 정의 네트워킹	• 소프트웨어 정의 네트워크 운영 지침 • SDN 아키텍처 및 네트워크 구성도 • SDN 컨트롤러 운영 현황 및 정책 설정 내역 • 트래픽 제어 및 정책 변경 관리 이력 • SDN 운영 현황 및 트래픽 분석 보고서

구분	기능	세부역량	증적 자료
네트워크	3.2 위협 대응	3.2.1 위협 대응	• 위협 탐지 및 대응 지침 • 위협 탐지 및 차단 시스템(IDS/IPS/SIEM 등) 운영 화면 • 침해사고 대응 및 조치 이력(탐지, 분석, 차단 로그) • 위협 인텔리전스(CTI) 연동 및 정책 반영 내역 • 보안관제 현황 및 위협 분석 보고서
	3.3 트래픽 암호화	3.3.1 트래픽 암호화	• 암호화 통제 및 키 관리 지침 • 네트워크 구간별 암호화 적용 현황(VPN, SSL/TLS 적용 대상 등) • 암호화 시스템(VPN/KMS 등) 운영 화면 • 인증서 및 암호화 키 관리 대장 • 암호화 정책 적용 및 점검 내역
	3.4 트래픽 관리	3.4.1 데이터 흐름 매핑	• 데이터 흐름 분석 및 관리 지침 • 데이터 흐름도(시스템/업무 단위 상세 흐름) • 트래픽 분석 및 모니터링 시스템(NMS/NDR 등) 운영 화면 • 비정상 트래픽 탐지 및 조치 로그
	3.5 네트워크 회복성	3.5.1 네트워크 회복성	• 재해복구(DR) 및 업무연속성(BCP) 관리 지침 • 네트워크 이중화 설계서 및 구성도 • 주요 시스템 백업 및 복구 현황 • 재해복구 모의훈련 계획 및 결과 보고서 • 장애 발생 및 복구 조치 이력(Failover 로그 등)
시스템	4.1 접근통제	4.1.1 접근통제	• 시스템 접근통제 정책 및 지침 • 시스템 접근권한 정의서(RBAC 매트릭스) • 접근제어 시스템(SSO/IAM/PAM 등) 운영 화면 • 시스템 접근 및 권한 부여 이력 • 접근권한 검토 및 점검 보고서
	4.2 시스템 계정 관리	4.2.1 PAM	• 특권 계정 및 접근통제 관리 지침 • 특권 계정(시스템/DB) 관리대장 • 특권 접근 관리(PAM) 시스템 운영 화면 • 권한 상승 신청·승인 및 접속 이력 • 특권 계정 사용 내역 점검 및 감사 보고서
		4.2.2 자격 증명 관리	• 자격 증명 및 인증 관리 지침(패스워드 작성 규칙, 갱신 주기 등) • 자격 증명 관리 시스템(MFA/ICAM 등) 운영 화면 • 자격 증명 발급·갱신·폐기 이력 • 비정상 인증 탐지 및 차단 로그 • 자격 증명 현황 및 보안 점검 보고서
	4.3 네트워크 분리 정책	4.3.1 네트워크 세분화 및 그룹 간 이동	• 네트워크 구성도(전체/영역별) • 네트워크 분리 및 접근통제 지침 • 네트워크 접근제어(ACL) 및 세분화 정책 설정 내역 • 세그먼트 간 접근통제 및 이상행위 차단 이력 • 네트워크 접근제어 정책 검토 및 점검 내역
	4.4 시스템 보안 및 정책 관리	4.4.1 시스템 환경에 따른 정책 관리	• 시스템 보안 관리 지침(온프레미스 및 클라우드 환경별 보안 정책 포함) • 하이브리드 클라우드 정책 연동 아키텍처(구성도) • 클라우드 보안 통합 관리 시스템(CNAPP 등) 운영 화면 • IaC(코드 기반 인프라) 스크립트 및 정책 템플릿 • 보안 정책 변경 및 자동 배포 이력(CI/CD 파이프라인 연동 로그) • DevSecOps 파이프라인 내 보안 정책 관련 정책 및 지침

구분	기능	세부역량	증적 자료
애플리케이션 및 워크로드	5.1 애플리케이션 접근	5.1.1 리소스 권한 부여 및 통합	• 애플리케이션 및 리소스 접근통제 지침 • 통합 계정권한관리 시스템(IAM/ICAM 등) 운영 화면 • 애플리케이션별 접근권한 정의서(RBAC/ABAC) • 권한 부여/회수 자동화 및 승인 이력 • 접근권한 정기 검토 및 조치 결과 보고서
	5.2 애플리케이션 위협 보호	5.2.1 지속적인 모니터링 및 진행 중인 승인	• 보안 모니터링 및 운영 지침 • 통합 보안 관제 시스템(SIEM/XDR 등) 운영 화면 및 대시보드 • 시스템 변경 보안성 검토 및 승인 내역(DevSecOps 파이프라인 연동 포함) • 이상 징후 탐지 및 대응 이력 • 보안 관제 정기(주간/월간) 보고서
	5.3 접근 가능한 애플리케이션	5.3.1 원격 접속	• 원격 접속 보안 관리 지침(인가 절차, 접근 단말 보안 기준 등) • 원격 접속 대상 및 접근권한 현황 목록 • 원격 접속 통제 시스템(VPN/ZTNA 등) 운영 화면 • 접근 단말 보안 설정 및 무결성 검증 내역 • 비정상 원격 접속 탐지 및 차단 이력
	5.4 안전한 애플리케이션 배포	5.4.1 안전한 애플리케이션 배포	• 소프트웨어 개발 보안 가이드 및 운영 지침 • SDLC(소프트웨어 개발 생명주기)기반 개발 및 운영 가이드 • CI/CD 파이프라인 보안(SAST/DAST/SCA 등) 설정 화면 • 애플리케이션 보안성 검토 및 취약점 조치 이력 • 배포 자동화 및 코드 무결성 검증 로그 • 배포 과정의 이상행위 탐지 및 대응 보고서
		5.4.2 애플리케이션 인벤토리	• 애플리케이션 자산관리 지침 • 애플리케이션 관리대장(개발자 및 담당자 지정) • 애플리케이션 자동 식별 및 관리 시스템(ITAM 등) 운영 화면 • 애플리케이션 변경 관리 및 현행화 이력 • 애플리케이션 보안 현황(취약점/패치) 점검 보고서
	5.5 소프트웨어·애플리케이션 보안	5.5.1 안전한 소프트웨어 개발 및 통합	• 소프트웨어 개발 보안 지침(시큐어코딩 표준 및 SDLC 단계별 보안 절차) • CI/CD 보안 자동화 시스템 설정 화면(SAST/DAST/SCA 연동 현황) • 소스코드 보안약점 진단 및 이행 조치서 • 오픈소스 점검 내역 및 SBOM 관리대장 • 개발·운영 환경 분리 및 접근통제 현황
		5.5.2 소프트웨어 위험 관리	• 소프트웨어 위험 관리 지침 및 계획서(위험 식별/평가/조치) • 소프트웨어 위험 식별 및 평가 보고서(취약점 등급 분류 및 우선순위 산정) • 소프트웨어 공급망(오픈소스/서드파티) 위험 분석 내역 • 위험 관리 시스템(취약점 진단/모니터링) 운영 화면 • 위험 조치 및 개선 결과 보고서

구분	기능	세부역량	증적 자료
데이터	6.1 데이터 목록 관리	6.1.1 데이터 카탈로그 위험 정렬	• 데이터 분류 및 위험 평가 지침 • 데이터 카탈로그 및 위험 등급 현황 목록 • 데이터 보안 형상 관리(DSPM) 시스템 운영 화면 • 데이터 위험 식별 및 자동 분류 이력 • 데이터 보안 위험 평가 및 조치 결과 보고서
		6.1.2 기업 데이터 거버넌스	• 데이터 거버넌스 정책 및 관리 지침(데이터 관리 원칙 포함) • 데이터 소유자 및 관리자 지정 내역(R&R 정의 문서) • 데이터 거버넌스 관리 시스템eDRM/eDLP/(DSPM 등) 운영 화면 • 데이터 정책 준수 모니터링 및 위반 처리 이력 • 데이터 거버넌스 이행 점검 및 감사 보고서
	6.2 접근 결정방법	6.2.1 데이터 접근제어	• 데이터 접근제어 정책 및 지침 • 데이터 접근권한 관리대장 • 데이터 접근제어 시스템(DBAM/PAM 등) 운영 화면 • 접근권한 부여·변경·해지 이력 • 접근권한 검토 및 조치 결과 보고서
	6.3 데이터 암호화	6.3.1 데이터 암호화 및 권한 관리	• 데이터 암호화 및 키 관리 지침 • 암호화 대상 목록(DB/문서 관리대장) • 암호화 시스템(DB암호화/eDRM/KMS 등) 운영 화면 • 암호화 키 관리 및 권한 제어 이력 • 표준 암호화 알고리즘 적용 및 API 연동 내역 • 암호화 적용 및 권한 점검 보고서
	6.4 데이터 분류	6.4.1 데이터 라벨링 및 태그 지정	• 데이터 분류 및 라벨링 관리 지침(등급별 라벨링 기준 및 태깅 규칙) • 데이터 라벨링 및 태그 지정 현황 목록 • 라벨링 자동화 도구(eDRM/eDLP/DSPM 등) 운영 화면 • 데이터 등급별 보호 정책 설정 및 연동 내역 • 라벨링 적용 적정성 검토 및 점검 보고서
	6.5 데이터 손실 방지	6.5.1 데이터 손실 방지(DLP)	• 데이터 유출 방지(DLP) 정책 및 지침 • 주요 정보 유출 경로별 통제 현황 목록 • 데이터 유출 방지 시스템(eDLP 등) 운영 화면 • 데이터 유출 탐지·차단 및 소명/조치 이력 • 데이터 유출 사고 분석 및 대응 결과 보고서
		6.5.2 데이터 모니터링 및 감지	• 데이터 모니터링 및 이상행위 탐지 절차 및 지침 • 통합 보안 모니터링 시스템(SIEM/UEBA 등) 운영 화면 • 데이터 이상행위 탐지 및 분석 이력 • 보안 위협 자동 대응 및 조치 내역 • 데이터 보안 모니터링 정기 결과 보고서

구분	세부역량	증적 자료
가시성 및 분석	7.1 모든 관련 활동 기록	• 로그 및 이벤트 관리 지침(수집 대상, 보존 기간, 무결성 확보 등) • 로그 수집 및 연동 현황 목록(SIEM 연동 여부) • 통합 로그 및 보안 관제 시스템(SIEM 등) 운영 화면 • 로그 무결성 검증 및 접근통제 이력 • 로그 분석 및 이상 징후 대응 보고서
	7.2 중앙집중적 보안 정보 및 이벤트 관리	• 보안 관제 및 사고 대응 지침 • 통합 보안 관제 시스템(SIEM 등) 운영 화면 • 보안 로그 연동 현황 및 상관 분석 규칙(Rule) 정의서 • 보안 위협 탐지 및 대응 이력(SOAR 연동 자동 대응 내용 포함) • 보안 관제 정기(주간/월간) 보고서
	7.3 보안 위협 분석	• 보안 위협 및 취약점 관리 지침 • 보안 위협 분석 시스템(빅데이터/UEBA/SIEM 등) 운영 화면 • 취약점 정보 수집 및 위험 평가(CVSS) 내역 • 위협 탐지 및 자동 경보 이력 • 보안 위협 분석 정기(주간/월간) 보고서
	7.4 사용자 및 기기 동작 분석	• 사용자 이상행위 탐지 및 대응 관리 지침 • 사용자 및 기기 행위 분석 시스템(ZTNA/XDR/UEBA 등) 운영 화면 • 사용자 및 기기 이상행위 탐지 시나리오/임계치 설정 내역 • 비정상 행위 탐지 및 자동 조치 이력 • 이상행위 분석 및 대응 결과 보고서
	7.5 위협 인텔리전스 통합	• 위협 인텔리전스 관리 지침 • 위협 인텔리전스 연동 현황 및 구성도(내·외부 포함) • 위협 인텔리전스 플랫폼(TIP) 운영 화면 • 위협 정보 기반 탐지 및 정책 적용 이력 • 위협 분석 및 대응 결과 보고서
	7.6 자동화된 동적 정책	• 동적 보안 정책 관리 및 운영 지침 • 동적 정책 자동화 연동 구성도 및 흐름도(시스템 간 연동 구조 및 정책 반영 절차) • 보안 정책 자동화 시스템 운영 화면 • 보안 이벤트 기반 정책 자동 변경 이력
자동화 및 통합	8.1 정책통합	• 정보보호 정책·지침·절차서(제·개정 내역 포함) • 통합 정책 관리 시스템(SIEM/SOAR/보안포털 등) 운영 화면 • 보안 정책 변경 신청 및 승인 내역(정책 변경 관리대장) • 정책 일괄 적용 및 동기화 이력(정책 배포 자동화 로그) • 보안 정책 정합성 점검 및 조치 결과 보고서
	8.2 중요 프로세스 자동화	• 주요 프로세스 자동화 관리 지침·절차서 • 자동화 시스템(RPA/SOAR 등) 운영 화면 • 데이터 백업 및 자동 복구 수행 내역 • 보안 이벤트 및 장애 자동 대응 로그 • 자동화 프로세스 운영 현황 및 결과 보고서
	8.3 인공지능	• AI 기반 보안 운영 및 자동화 관리 지침 • 개별 보안 시스템(IAM/EDR/XDR/ZTNA 등) AI 탐지 설정 내역 (단위 솔루션의 ML 기능 적용 현황) • 통합 분석 시스템(UEBA/ICAM/SIEM/SOAR 등) AI 모델 운영 화면 (중앙 집중식 학습 및 분석 현황) • AI 기반 위협 예측 및 자동 대응 이력 • AI 보안 관제 및 운영 효율성 분석 보고서

구분	세부역량	증적 자료
자동화 및 통합	8.4 보안 통합, 자동화 및 대응	• 보안 통합 및 자동화 대응 운영 지침 • 보안 시스템 연동 구성도 및 대응 흐름도 • 보안 오케스트레이션(SOAR) 시스템 운영 화면 • 보안 위협 자동 탐지 및 대응(플레이북 실행) 이력 • 보안 사고 통합 대응 결과 보고서
	8.5 데이터 교환 표준화	• 데이터 교환 표준화 정책 및 지침 (데이터 포맷, 연동 프로토콜 표준 정의) • 데이터 연동 현황 및 구성도 • 데이터 교환 및 연계 시스템(WAAP/API 게이트웨이 등) 운영 화면 • 데이터 교환(전송/수신) 자동화 처리 로그 • 데이터 정합성 검증 및 연동 오류 조치 내역
	8.6 보안 운영 조정 및 사고 대응	• 보안사고 대응 정책 및 표준운영절차(SOP) • 보안사고 대응 조직도 및 비상연락망 • 사고 대응 자동화 시스템(SOAR) 운영 화면(대시보드, 워크플로우 설정) • 보안사고 탐지 및 대응 조치 이력 (자동화/수동 조치 로그) • 보안사고 분석 및 재발방지 대책 보고서

3. 용어 정의

용어	정의
기능 (Function)	• 어떤 일이나 목적, 요구사항을 달성하기 위해 필요한 능력 • 제로트러스트 성숙도 모델 2.0에서 정의하는 기능은, 기업망에서 제로트러스트 아키텍처를 구현하는 데 있어서 필요한 보안 능력을 의미
기업 데이터 거버넌스 (Enterprise Data Governance)	• 조직 내 모든 데이터의 사용, 보호, 관리에 대한 규칙과 절차를 정의하고, 이를 준수하는 과정
네트워크 회복성 (Network Resilience)	• 네트워크가 다양한 위협이나 장애로부터 신속하게 복구하고, 지속적으로 가용성을 유지할 수 있도록 하는 능력
데이터 카탈로그 (Data Catalog)	• 조직의 모든 데이터를 분류하고, 데이터가 식별 및 목록화되고 데이터 환경에 대한 모든 변경 사항이 자동으로 감지되어 카탈로그 내에 포함되는지 확인하는 것
리소스 (Resource)	• 데이터를 포함하여 기업망 내부에서 보호 대상이 되는 모든 종류의 디지털 자산을 의미하며, 데이터 외에도 프린터, 컴퓨팅 리소스, IoT 액추에이터 등을 포함하기도 함
비인간개체 (NPE,·Non-Person·Entity)	• 기업망에서 사용자가 아닌 기기, 서버, 애플리케이션, 서비스 등으로 특정 리소스에 접근하는 접근 주체 역할을 수행 할 수 있으며, 이 경우 신원 확인 및 권한 검증, 신뢰도 확인 등이 이루어져야 함
사용자 인벤토리 (User Inventory)	• 시스템에 접근하는 모든 사용자와 그들의 권한을 기록하고 관리하는 시스템
세부역량 (Capability)	• 일련의 작업을 수행하기 위한 수단과 방법의 조합을 통해 원하는 요구사항 혹은 효과를 달성할 수 있는 능력 및 이를 바탕으로 구현되는 구체적 기능
워크로드 (Workload)	• 기업망에서 시스템, 애플리케이션 등이 처리해야 하는 작업 혹은 일련의 작업 리스트 등을 의미하며, 제로트러스트 관점에서는 온프레미스 혹은 클라우드에 위치한 리소스에 접근하는 모든 서비스, 애플리케이션 및 솔루션 등을 포괄
위협 인텔리전스 통합 (Threat Intelligence Integration)	• 외부의 보안 위협 정보를 수집하고 이를 조직 내 보안 시스템에 적용하여 위협 대응 능력을 향상 시키는 기능
접근 (Access)	• 접근 주체가 리소스를 이용하는 과정으로, 단순히 데이터를 읽는 것 뿐만 아니라, 수정, 삭제 및 데이터 이외의 디지털 자산에 데이터를 전송하거나 전송받는 등의 행위를 포함
접근 주체 (Subject)	• 사용자와 애플리케이션(혹은 서비스), 기기의 조합이며, 여기에 악의적인 공격자 혹은 불법적인 애플리케이션, 감염된 기기 등이 포함될 수 있음
정책결정지점 (PDP, Policy Decision Point)	• 접근 주체가 리소스에 접근할 수 있는지를 최종적으로 결정하여 이를 정책시행지점(PEP)에게 명령하는 논리적 개체로, 정책 엔진(PE)과 정책 관리자(PA)로 구성

정책 관리자 (PA, Policy Administrator)	• 접근 주체와 리소스 사이의 통신 경로를 생성하거나 취소하기 위한 결정을 정책 시행지점(PEP)에게 전달하는 논리 개체
정책 엔진 (PE, Policy Engine)	• 접근 주체가 리소스에 접근할 수 있는지를 최종적으로 결정하는 논리적 개체로, 정책정보 지점(PIP)으로부터 신뢰도를 평가할 수 있는 알고리즘에 대한 입력을 수신하여, 현재 리소스 접근 요청을 승인하거나 거부 혹은 현재 연결 중인 상태의 접근을 취소할 수 있음
정책시행지점 (PEP, Policy Enforcement Point)	• 접근 주체와 리소스 사이를 연결하고 모니터링하며 최종적으로 연결을 종료하는 논리적 개체로, PDP의 정책 관리자에게 접근 요청을 전달하고 접근 승인 여부를 전달받아 현재 접근 세션에 직접 반영
정책정보지점 (PIP, Policy Information Point)	• 정책결정지점이 정책 결정을 내리는 데 활용하기 위해서 수집한 사용자, 기기 관련 정보 및 기타 정책 관련 정보를 제공하는 논리적 개체로, 이러한 정보에는 기업이 생성하거나 제어하지 않는 외부 데이터와 기업 내부적으로 생성되는 내부 데이터로 분류할 수 있으며 규제·내부규정, 데이터 접근 정책, 보안 이벤트, 위협 인텔리전스, 사용자 및 기기 인증 정보, 네트워크 및 시스템상의 행위 로그 등을 포함할 수 있음
제로트러스트 (Zero Trust)	• 위협이 언제 어디서든 발생 가능하다는 인식하에 기업 내부의 네트워크, 시스템 혹은 리소스에 접근하고자 하는 어떤 사용자·기기에 대해서도 지속 인증, 세밀한 접근제어를 통한 최소 권한 부여 등 적극적인 신뢰도 평가 없이 접근을 허용하지 않는 보안 모델 및 이를 구현·실체화하기 위한 아이디어의 집합을 의미 • 영어 원문을 발음대로 쓴 표현으로 두 단어의 결합인 점을 고려하면 '제로트러스트'라고 표현할 수 있으나, 이 문구가 '제로(무)'와 '트러스트(신뢰)'의 단순 단어 결합이 아닌 새로운 보안 모델로서의 의미를 담고 있음을 고려하고 독자들이 해당 의미를 받아들이는 데 도움이 될 수 있도록 본 가이드라인에서는 두 단어를 붙인 형태의 새로운 단어로 표현하고 있음
제로트러스트 아키텍처 (Zero Trust Architecture)	• 제로트러스트의 개념을 활용하여 기업 내부의 네트워크, 시스템 및 리소스를 보호할 수 있는 추상적인 보안 구조이며 해당 목적을 달성하기 위한 기업망의 구성 요소, 구성 요소 간 인터페이스 정의와 인증, 접근제어, 보안 모니터링 및 가시화 등 보안 정책을 포함
컨텍스트 (Context)	• 특정 접근 주체가 리소스에 접근할 때 접근제어 및 신뢰도 평가에 있어 활용될 수 있는 모든 상황 정보를 의미하며, 이러한 정보에는 사용자의 신원, 기기 상태 및 위치, 사용자의 실행 애플리케이션, 접속 시간, 접근하고자 하는 리소스, 네트워크 상태 등을 포함할 수 있음 • 제로트러스트 성숙도 수준이 높아질 경우 가급적 많은 컨텍스트 정보를 실시간으로 확보하여 현재 접근 요청에 대해 동적으로 신뢰도를 판단하기 위해 사용함
퀵윈 (Quick-win)	• 짧은 시간 안에 가시적인 성과를 낼 수 있는 과제를 찾아 실행하는 전략 • 단기적인 성공을 통해 조직 구성원의 사기를 높이고, 장기적인 혁신을 위한 동력을 얻는 데 목적이 있음
프로비저닝 (Provisioning)	• 기업망에서 사용자, 기기 등이 서비스를 받기 위해 필요한 리소스 및 이에 대한 접근권한, 정책 등을 사전에 준비하고 배포하는 절차 및 과정을 의미

출처: KISA, 제로트러스트 가이드라인 2.0

4. 약어 정의

- **ABAC** Attribute-Based Access Control
- **ACL** Access Control List
- **AD** Active Directory
- **AI** Artificial Intelligence
- **AP** Access Point
- **AV** Anti-Virus
- **BCP** Business Continuity Plan
- **BGP** Border Gateway Protocol
- **BYOD** Bring Your Own Device
- **C&C** Command & Control
- **CVE** Common Vulnerabilities and Exposures
- **DLP** Data Loss Prevention
- **DR** Disaster Recovery
- **DRM** Digital Rights Management
- **eDLP** Enterprise Data Loss Prevention
- **eDRM** Enterprise Digital Rights Management
- **ECDHE** Elliptic Curve Diffie-Hellman Ephemeral
- **EDR** Endpoint Detection & Response
- **EPP** Endpoint Protection Platform
- **ERP** Enterprise Resource Planning
- **FIDO** Fast IDentity Online
- **FIM** File Integrity Monitoring
- **GPO** Group Policy Object
- **HRM** Human Resource Management
- **HTTPS** Hyper Text Transfer Protocol Secure

- **IAM** Identity and Access Management
- **IAST** Interactive Application Security Testing
- **ICAM** Identity, Credential and Access Management
- **IDP** Identity Provider
- **IDS** Intrusion Detection System
- **ILM** Identity Lifecycle Management
- **IoT** Internet of Things
- **IOA** Indicator of Attack
- **IOC** Indicator of Compromise
- **IPS** Intrusion Protection System
- **ITAM** IT Asset Management
- **JIT/JEA** Just-In Time/Just-Enough Access
- **KMS** Key Management System
- **LACP** Link Aggregation Control Protocol
- **LEEF** Log Event Extended Format
- **MAC** Message Authentication code
- **MAM** Mobile Application Management
- **MDM** Mobile Device Management
- **MDR** Managed Detection and Response
- **MFA** Multi-Factor Authentication
- **ML** Machine Learning
- **MTTR** Mean Time To Respond
- **NAC** Network Access Control
- **NGFW** Next-Generation Firewall
- **NMS** Network Management System
- **NSA** National Security Agency
- **NSG** Network Security Group
- **OAuth** Open Authorization

- **OIDC** OpenID Connect
- **OSINT** Open-Source Intelligence
- **OSPF** Open Shortest Path First
- **OT** Operation Technology
- **OTP** One Time Password
- **OWASP** Open Web Application Security Project
- **PAM** Privileged Access Management
- **PHI** Protected Health Information
- **PII** Personally Identifiable Information
- **PKI** Public Key Infrastructure
- **PMS** Patch Management System
- **PQC** Post-Quantum Cryptography
- **QENC** Quantum-Communication Encrypted Device
- **QKD** Quantum Key Distribution
- **QoS** Quality of Service
- **RBAC** Role-Based Access Control
- **RIP** Routing Information Protocol
- **ROI** Return on Investment
- **RPA** Robotic Process Automation
- **SaaS** Software as a Service
- **SAML** Security Assertion Markup Language
- **SBOM** Software Bill of Materials
- **SDLC** Software Development LifeCycle
- **SDN** Software Defined Networking
- **SDP** Software Defined Perimeter
- **SIEM** Security Information and Event Management
- **SOAR** Security Orchestration, Automation and Response
- **SOC** Security Operation Center

- **SSH** Secure Shell
- **SSL** Secure Sockets Layer
- **SSO** Single Sign On
- **STP** Spanning Tree Protocol
- **TI** Threat Intelligence
- **TLS** Transport Layer Security
- **UEBA** User and Entity Behavioral Analytics
- **UEM** Unified Endpoint Management
- **VDI** Virtual Desktop Infrastructure
- **VM** Virtual Machine
- **VPC** Virtual Private Cloud
- **VPN** Virtual Private Network
- **WAPP** Web Application & API Protection
- **WORM** Write Once Read Many
- **XDR** eXtended Detection & Response
- **XML** eXtensible Markup Language
- **ZTNA** Zero Trust Network Access

집필진

- 투이컨설팅 정관복 이사
- 투이컨설팅 김도형 이사
- 투이컨설팅 김병민 컨설턴트
- 투이컨설팅 이봉학 컨설턴트
- SK쉴더스 이봉준 수석
- SK쉴더스 황병권 책임
- SK쉴더스 김혜지 선임

연구반

- 가천대학교 이석준 교수
- 강남대학교 박정수 교수
- 국민대학교 김환국 교수
- 국가보안기술연구소 이택규 책임
- 에스지에이솔루션즈㈜ 최영철 대표
- 프라이빗테크놀로지㈜ 김주태 전무
- ㈜당근마켓 이원규 팀장
- 공항철도㈜ 안동원 팀장
- 한국정보보호산업협회(KISIA) 정호준 단장
- 한국인터넷진흥원(KISA) 하병욱 팀장
- 한국인터넷진흥원(KISA) 최슬기 선임연구원

End of Document