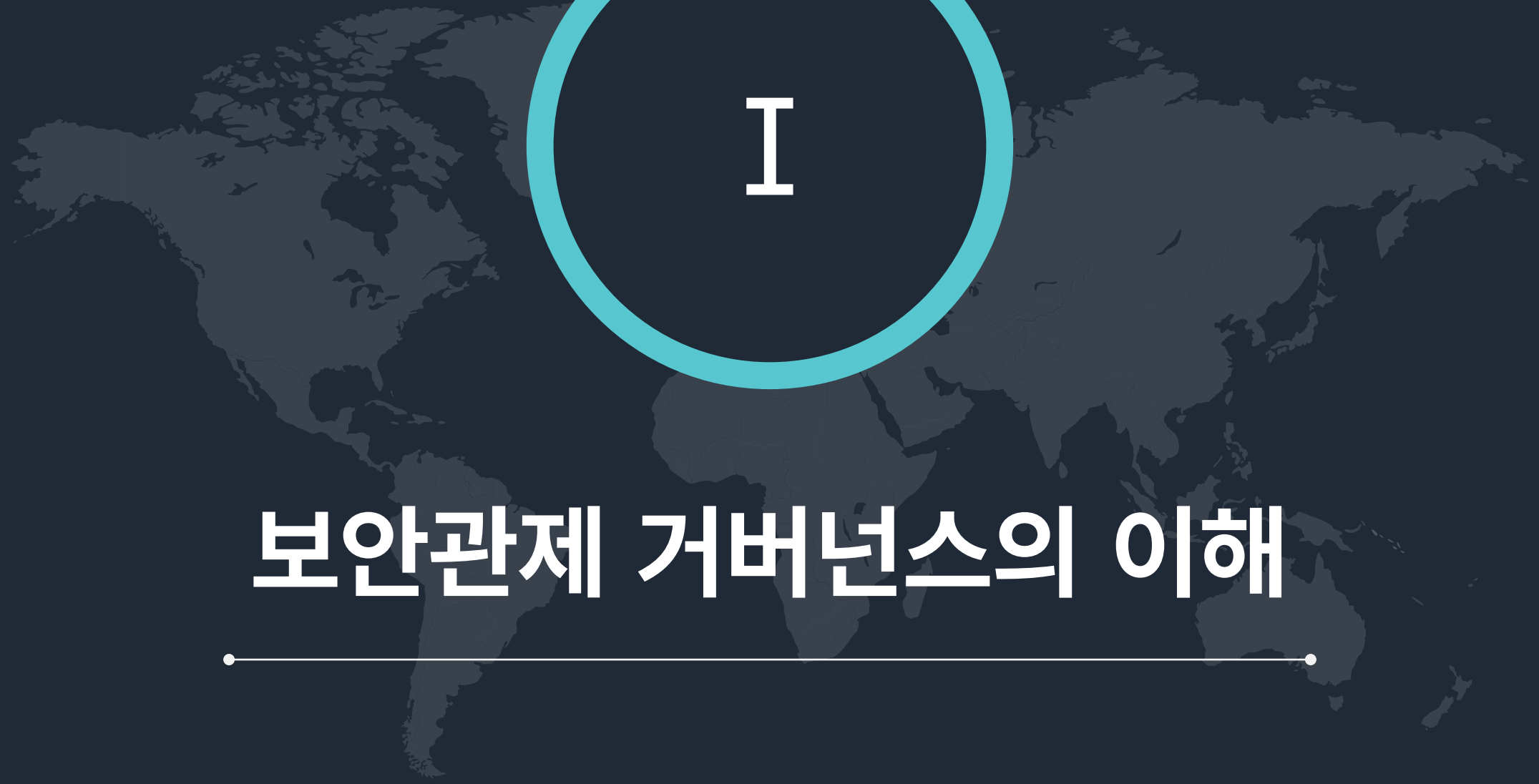
CHAPTER 02

보안관제 거버넌스와 방법론

이현호 hyeonholee@korea.com

목차

- 보안관제 거버넌스의 이해
- 보안관제의 유형과
  보안운영 조직 구성
- 보안관제 방법론과 프로세스
- 보안관제 관련 프레임워크



I

보안관제 거버넌스의 이해

I 보안관제 거버넌스의 이해

1 거버넌스(Governance)

- **조직이 조직의 목표를 추구하는 데 의사결정을 내리고 그 의사결정을 실행하는 체계 (ISO 26000)**
  - 조직이 어떤 목표를 달성하기 위해 제반 활동을 조정 · 통제 · 관리하는 체계와 프로세스
  - 조직의 전략 · 정책 · 절차를 설정하는 것과 이를 이행하는 방식에 관한 것을 포함

출처 사회적책임에 대한 지침(KS A ISO 26000:2010), 2021, 산업표준심의회, p. 22

보안관제 거버넌스의 이해

1 거버넌스(Governance)

- **거버넌스는 오늘날 조직의 운영 및 관리에 중요한 개념으로 작용**

  예 ESG 경영 : E(Environmental), S(Social), **G(Governance)**

  예 정보보호 GRC : **G(Governance)** R(Risk) C(Compliance)

출처 사회적책임에 대한 지침(KS A ISO 26000:2010), 2021, 산업표준심의회, p. 22

보안관제 거버넌스의 이해

2 보안관제 거버넌스

보안관제 거버넌스

보안관제에 대한 **의사결정 체계**

- **효과적인 위험 관리**
- **일관된 보안 프로세스와 정책**
- **책임 및 투명성 확보**
- **법적 요구사항 충족 및 규제 준수**

보안관제 거버넌스의 이해

3 보안관제 거버넌스의 필요성

- **효과적인 위험관리**
  - 조직에 대한 사이버보안 위험을 체계적으로 식별 · 평가 · 관리하며,
    신속하고 효과적인 대응을 위한 기반 마련
- **일관된 보안 프로세스와 정책**
  - 프로세스와 정책이 일관성 있고 체계적으로 실행되도록 보장하여
    보안관제의 효율성을 높이고 보안사고에 대한 대응력 강화
- **책임 및 투명성 확보**
  - 조직 내 역할과 책임을 명확히 하여 보안사고 발생 시 투명한 대응을 가능하게 하며
    조직 내 · 외부의 신뢰 구축에 기여
- **법적 요구사항 충족 및 규제 준수**
  - 관계 법령 및 방침에서 정하는 요구사항 및 규제 충족을 위해 필수적

보안관제 거버넌스의 이해

4 보안관제 수행 방식과 거버넌스

- 24시간 365일 보안관제는 조직의 사이버보안을 강화할 수 있으나
  많은 인력 · 비용 · 자원이 투입되는 만큼,
  조직의 규모 · 자원 · 특성에 따라 적절한 수행 방식을 결정해야 할 필요성

보안관제 수행 방식에 따라 보안관제 거버넌스에 영향

II

보안관제의 유형과 보안운영 조직 구성

II 보안관제의 유형과 보안운영 조직 구성

1 수행 방식에 따른 보안관제 유형 분류

자체(인하우스) 보안관제

직접 보안관제

자체 시설과 자체 인력 활용

외주(아웃소싱) 보안관제

파견 보안관제

자체 시설을 두되,
보안관제 전문 업체 인력 활용

원격 보안관제

보안관제 전문 업체의 시설과 인력 활용

2 자체(인하우스) 보안관제

- 조직 규모가 크거나 많은 정보 자산과 중요 정보를 취급하는 경우 자체 보안관제가 유리
- 자체 보안관제를 인하우스 보안관제라고도 하며, 직접 보안관제가 대표적인 수행 방식

직접 보안관제

- 자체 보안관제 시설을 구축하고 자체 인력을 기반으로 운용하는 방식
- 내부의 기밀 유지와 신속한 사고 처리에 초점
- 보안관제 기술을 자체 보유할 수 있고 업무의 연속성 보장

II 보안관제의 유형과 보안운영 조직 구성

2 자체(인하우스) 보안관제

이점	• 조직의 요구사항을 고려한 맞춤식 보안관제 체계 구축 가능 • 보안 이벤트와 대응에 대한 직접적인 관리 및 통제 강화 • 조직 내 데이터가 외부로 유출되지 않도록 기밀성 유지 가능
한계	• 자체 조직과 설비를 구축하고 유지하는데 많은 비용 발생 • 전문 보안 인력을 채용하고 지속적인 커리어 개발 요구 • 최신 보안 위협에 대응하기 위한 기술 업데이트 및 자원 투입 등 지속적인 유지 노력 필요

3 외주(아웃소싱) 보안관제

- 조직 규모가 작거나 비용 투자 및 인력 확보 등 부담을 낮추는 경우 외주 보안관제가 유리
- 외주 보안관제를 아웃소싱 보안관제라고도 하며, 파견 보안관제와 원격 보안관제로 구분

파견 보안관제

- 자체 보안관제 시설을 구축하되, 조직은 보안관제 전문 업체의 인력을 파견 받아 운영하는 방식
- 보안관제 전문 업체의 보유 기술력과 노하우 활용 가능

원격 보안관제

- 자체 보안관제 시설을 구축하지 않고 보안관제 전문 업체의 보안관제 체계를 그대로 사용하는 방식
- 최소의 비용으로 보안관제 전문 업체의 보안관제 체계와 인력 활용 가능

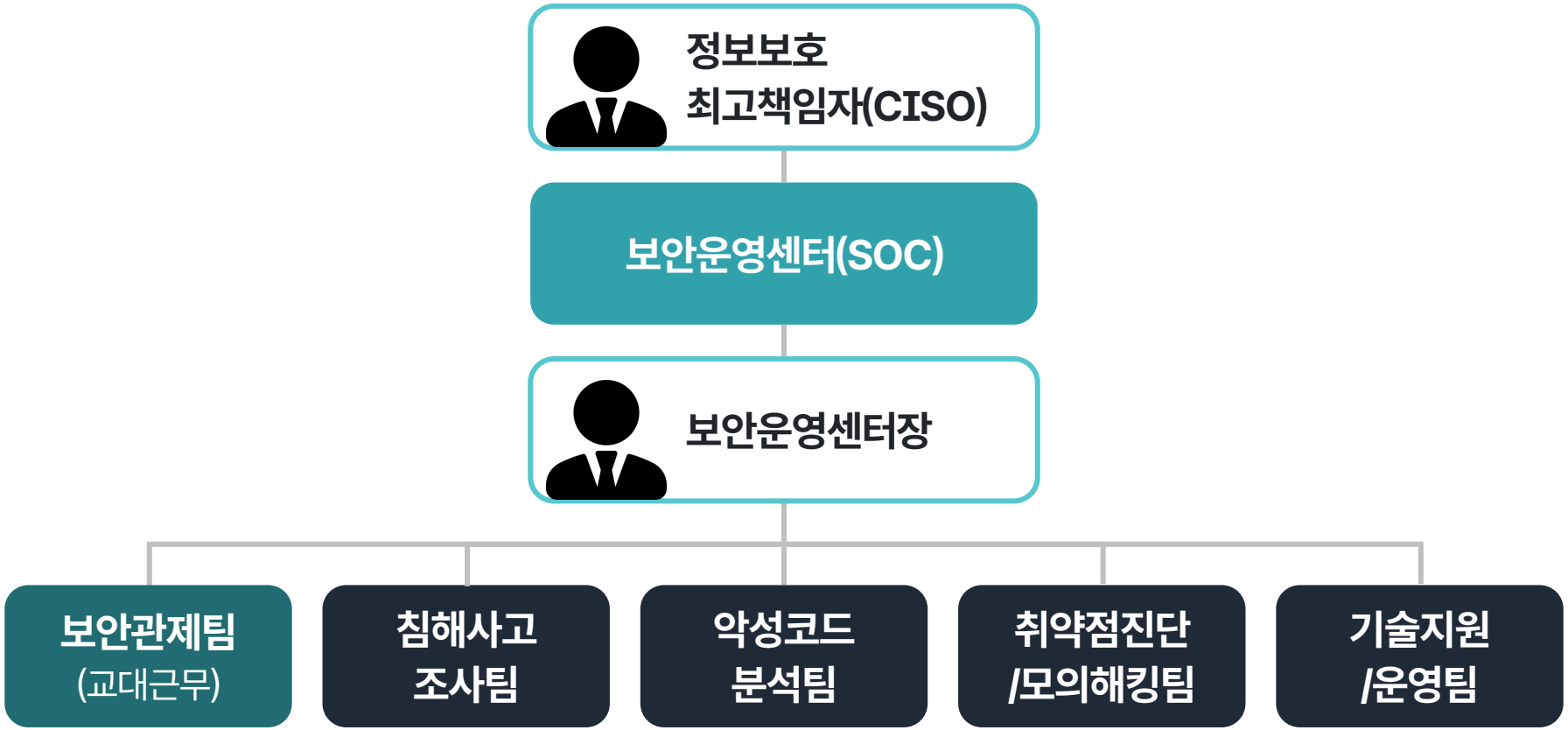
보안관제의 유형과 보안운영 조직 구성

3 외주(아웃소싱) 보안관제

이점	• 자체 조직과 설비 구축에 비해 저렴할 수 있고, 고정된 예산으로 관리 가능하여 효율적인 비용 운영 • 전문 조직 및 전문가의 지식과 경험 등 전문성을 즉각 활용 가능 • 조직 상황과 관계없이 항상 일정 수준의 보안관제 서비스 담보
한계	• 보안관제 전문 업체의 자원 및 접근방식을 따르므로 조직의 요구사항에 대한 맞춤화 제한 • 조직 내 데이터가 일정 부분 보안관제 전문 업체와 공유되므로 데이터 유출 우려 • 보안관제 전문 업체와의 의사소통 문제 발생 가능성

보안관제의 유형과 보안운영 조직 구성

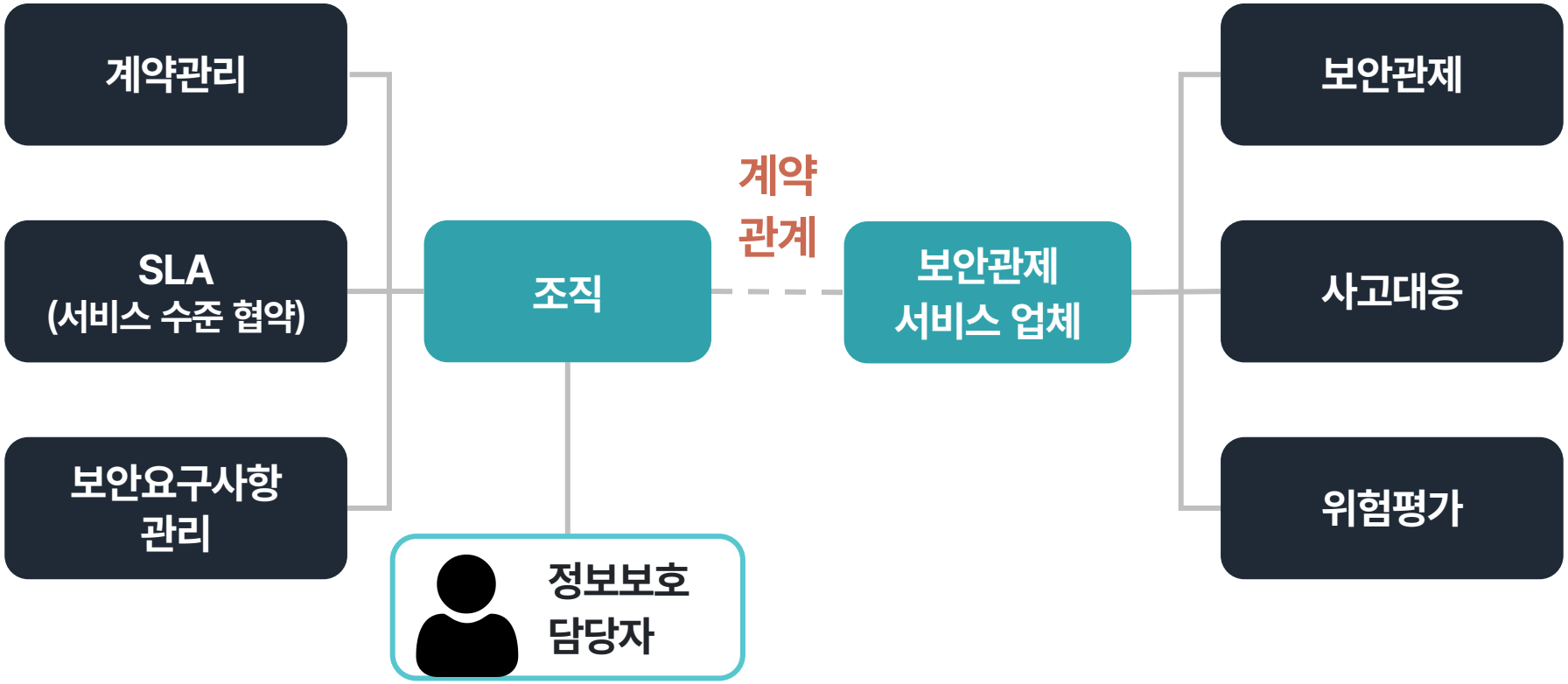
4 자체(인하우스) 보안운영 조직



4 자체(인하우스) 보안운영 조직

- **경영진의 감독 및 지원**
  - 정보보호 최고책임자는 전사 차원에서의 보안 전략과 정책을 주도하며, 보안관제 조직의 활동을 감독 · 지원
- **정책 및 절차**
  - 보안운영센터는 조직의 보안 정책과 절차에 따라 구성될 수 있으며, 보안관제를 자체 수행하는 경우 보안관제 기능을 포함
- **책임 및 역할 분담**
  - 보안운영센터의 효율적인 운영과 명확한 의사소통을 보장하기 위해 조직 내 책임 및 역할을 명확히 정의

5 외주(아웃소싱) 보안운영 구조



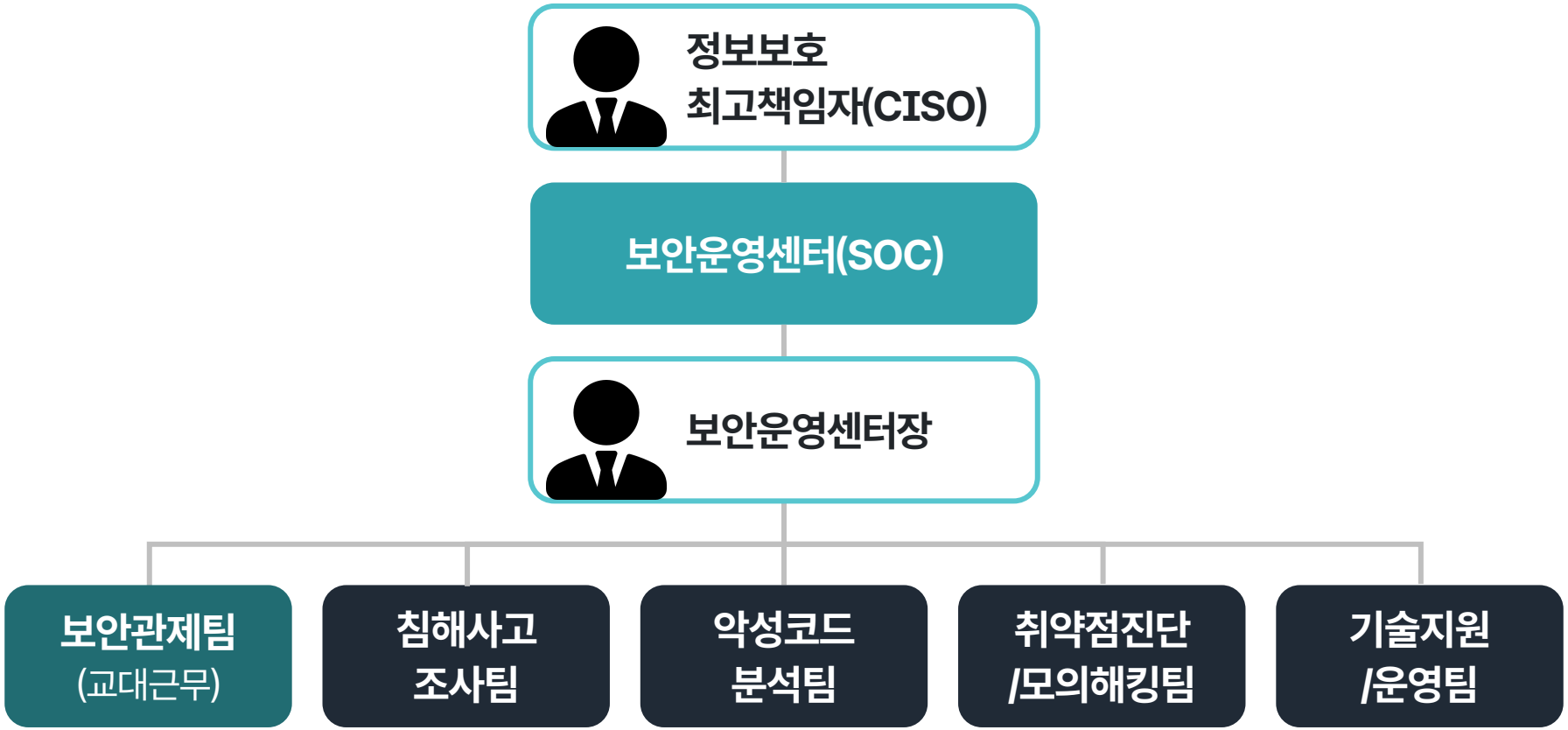
5 외주(아웃소싱) 보안운영 구조

- **외주(아웃소싱) 보안운영은 자체(인하우스) 보안운영 조직과는 달리, 계약 관계에 따른 협약 및 협력 구조를 취한다는 특징**

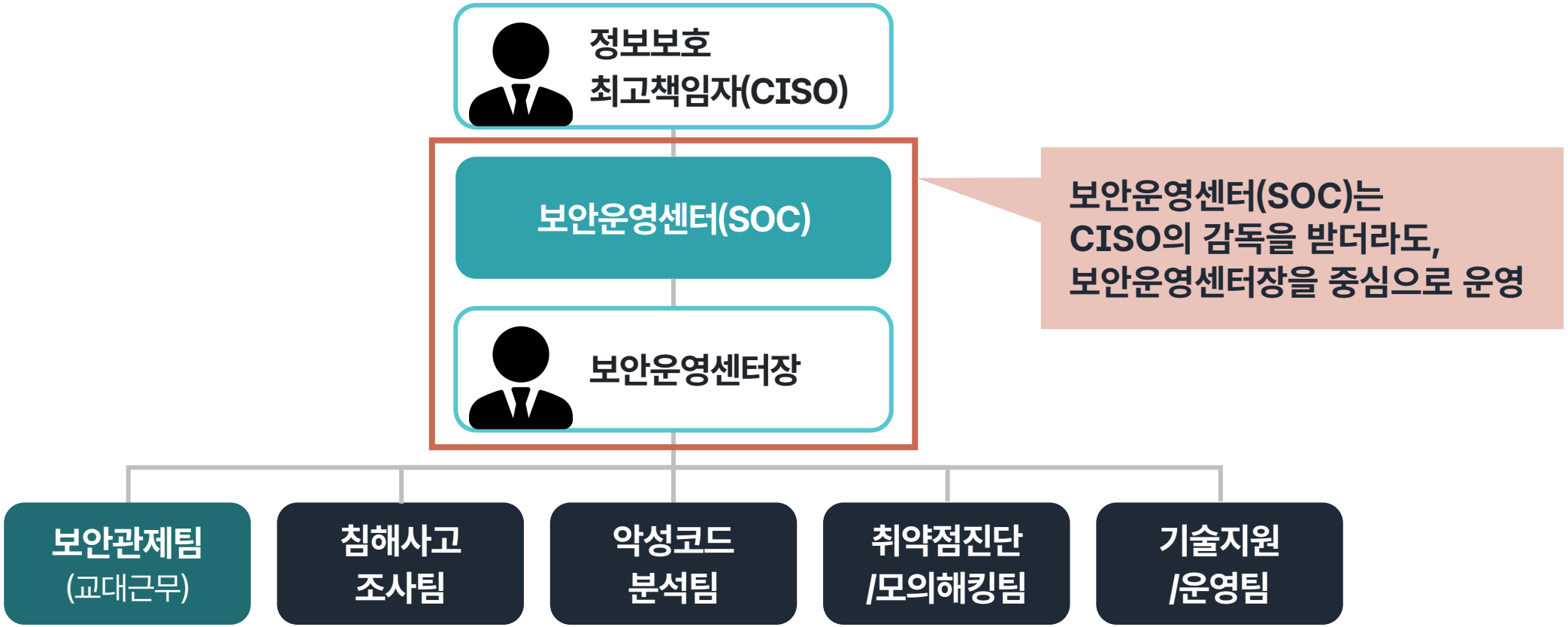
- **정책 및 절차**
  - 조직은 보안관제 서비스 업체와의 계약 및 협업을 관리하기 위한 내부 정책과 절차를 마련
- **서비스 수준 협약(Service Level Agreement, SLA)**
  - 보안관제 서비스 업체의 품질과 보안 효과를 주기적으로 검토하고 필요에 따라 조정
- **보안사고 발생 시 협력 대응**
  - 보안사고 발생 시 보안관제 서비스 업체와의 협력을 통해 적절한 대응을 수행

보안관제의 유형과 보안운영 조직 구성

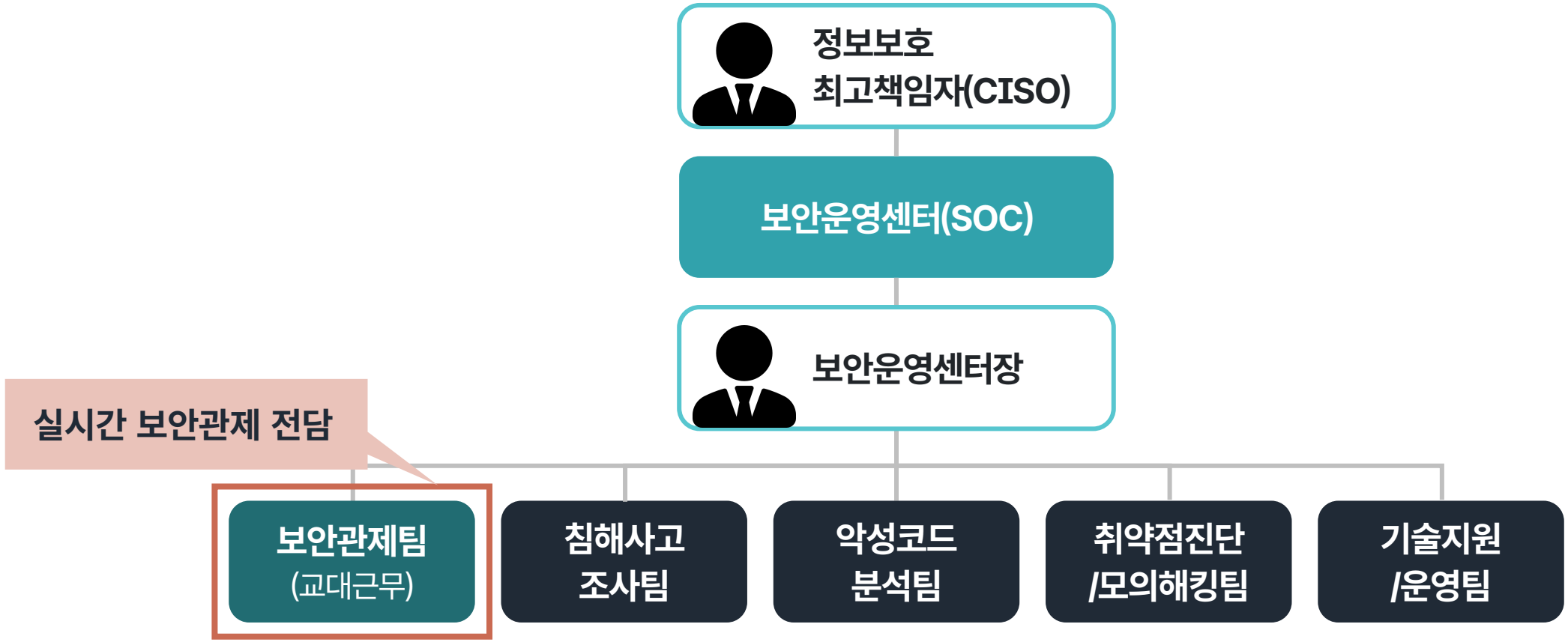
6 보안운영센터의 업무 분장



6 보안운영센터의 업무 분장

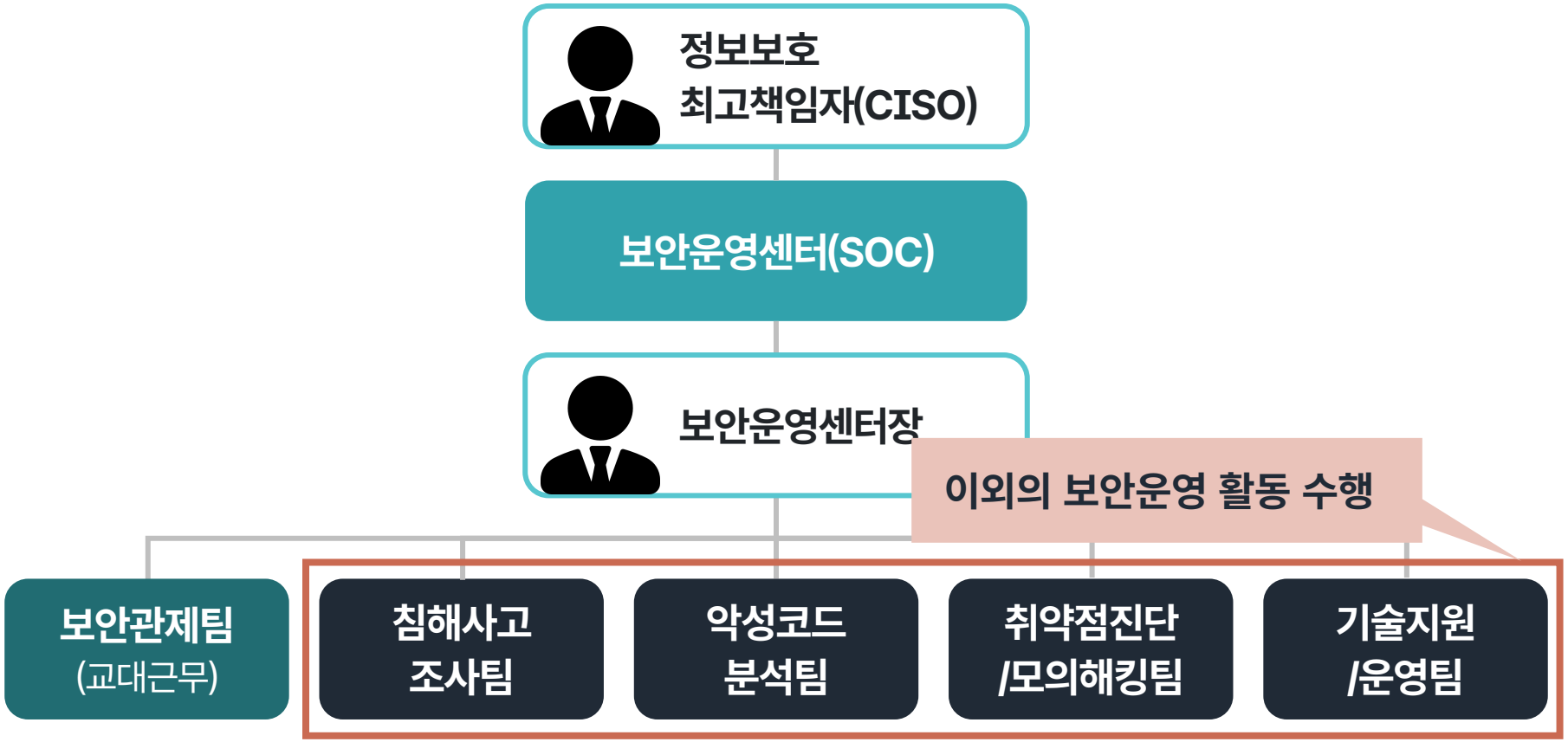


6 보안운영센터의 업무 분장



보안관제의 유형과 보안운영 조직 구성

6 보안운영센터의 업무 분장



6 보안운영센터의 업무 분장

- **보안운영센터장**
  - 보안운영센터의 일상적인 운영을 관리하고, 경영진에 의해 전사적으로 결정된 보안 전략 및 정책 이행
- **보안관제팀**
  - 보안 이벤트를 24시간 실시간 모니터링하고 식별된 보안 이벤트를 분석함으로써 보안 위협에 대응
- **조사분석팀** (침해사고조사, 악성코드분석)
  - 발생된 침해사고를 조사하고 채증된 악성코드 샘플 등을 분석하여 원인을 규명하고 재발방지 대책 강구
- **취약점진단/모의해킹팀**
  - 조직 정보통신망 및 정보시스템 내 정보자산에 내재될 가능성이 있는 취약점을 식별
- **기술지원/인프라운영팀**
  - 보안관제에 필요한 기술 및 정책관리 등을 지원하고 시스템에 대한 유지관리 및 운영을 지원

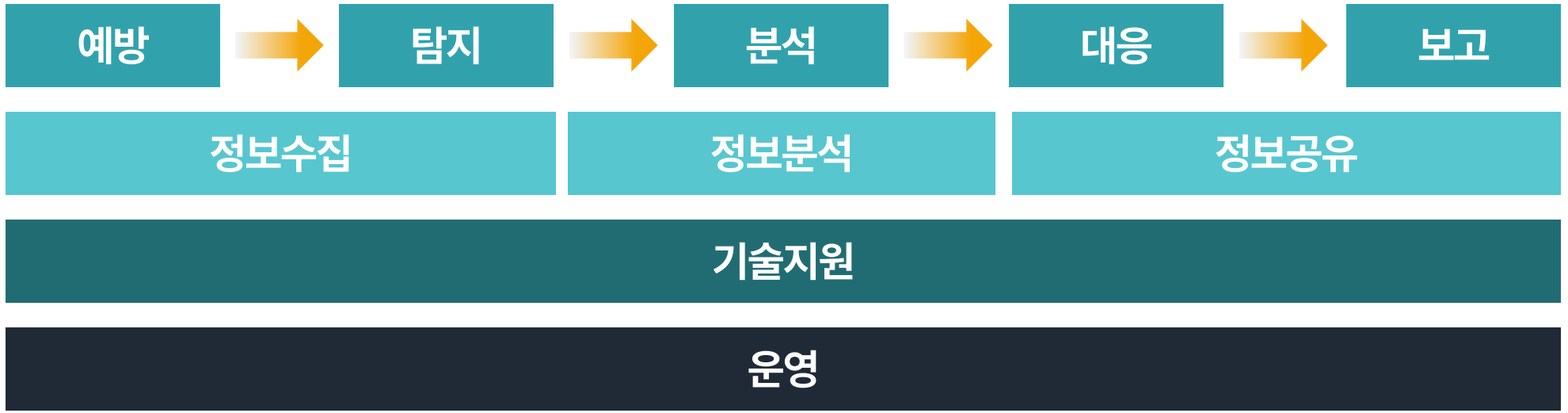
III

보안관제 방법론과 프로세스

1 보안관제 주요 활동

- 기본 활동

- 확장된 활동



2 확장된 활동에 따른 방법론

예방 → 탐지 → 분석 → 대응 → 보고

자산 식별 및 관리	• 정보통신망 및 정보시스템을 구성하는 정보자산을 식별하고 관리하는 업무
취약점 진단	• 정보통신망 및 정보시스템에 대한 알려진 보안취약점을 파악하는 업무
모의해킹	• 정보통신망 및 정보시스템에 대한 공격표면을 확인하고, 내재되어 있을 가능성이 있는 잠재적 보안취약점을 식별하는 업무
보안 패치	• 정보자산에 대한 알려진 보안취약점을 제거하는 업무
보안운영 정책 관리	• 방화벽, IDS/IPS 등 정보보호체계에 보안운영 정책(규칙)을 적용하는 업무

2 확장된 활동에 따른 방법론

예방 → **탐지** → 분석 → 대응 → 보고

- 365일 24시간 모니터링을 통해 위협 이벤트, 장애 이벤트, 관리적 이벤트 탐지

위협 이벤트 탐지	• 해킹, 침해시도, 침해사고 등 보안위협 이벤트를 탐지하는 업무
장애 이벤트 탐지	• 통신 마비, 시스템 오류, 성능 저하 등 장애 이벤트를 탐지하는 업무
관리적 이벤트 탐지	• 기타 관리에 필요한 각종 이벤트를 탐지하는 업무

2 확장된 활동에 따른 방법론

예방 → 탐지 → **분석** → 대응 → 보고

초기 분석	• 보안관제 수준에서 이벤트를 빠르게 분석하여 정탐/오탐 여부와 추가적인 조사 · 분석 필요성 등 대응 방책을 판단하는 업무 ✓ 오탐 → 자체 종결 ✓ 정탐 → 경중에 따라 대응 방책 판단
침해사고 조사	• 발생된 침해사고에 대해 정보자산으로부터 침해사고 흔적을 채증하거나 디지털 포렌식 등의 방법으로 조사하는 업무
악성코드 분석	• 채증된 악성코드 샘플을 역공학(Reverse Engineering) 등의 수단을 활용하여 정밀하게 분석하는 업무

2 확장된 활동에 따른 방법론

예방 → 탐지 → 분석 → **대응** → 보고

상황전파	• 피해 정보자산과 관련된 조직에 관련 사항을 통보하는 업무
인터뷰	• 피해자를 대상으로 경위(사용 행위 등) 확인 등 인터뷰를 시행하는 업무
차단 및 격리	• 피해 정보자산을 정보통신망에서 분리하고 격리 조치하는 업무
보안운영 정책 개발	• 정보보호체계에 적용하기 위한 보안운영 정책(규칙)을 개발하는 업무
복구	• 피해 정보자산을 정상 상태로 복구하여 조직의 업무 연속성 보장

2 확장된 활동에 따른 방법론

예방 → 탐지 → 분석 → 대응 → 보고

조직 내 보고	• 조직 내 보안 관련 의사결정권자에게 관련 사항을 보고하는 업무
유관기관 신고	• 경찰 등 정보수사기관에 침해사고 및 피해 사실을 신고하는 업무
조직 내 공유(공지)	• 조직 내 인식수준을 맞추고 향후 재발방지 등을 위한 전사 공지
사이버위협정보(CTI)	• 정보공유 업무와 연계하여 알려진 위협으로 생산 · 공유

2 확장된 활동에 따른 방법론

내부 위협정보 수집 (내부 위협 헌팅)	• 조직 내 정보통신망 및 정보시스템에 내재될 수 있는 보안 위협정보를 수집하는 업무
외부 위협정보 수집 (외부 위협 헌팅)	• 인터넷을 통해 광범위하게 유포되고 있는 보안 위협정보를 수집하는 업무

2 확장된 활동에 따른 방법론

예방	탐지	분석	대응	보고
정보수집		정보분석	정보공유	

위협정보 분석	• 자동화 분석 시스템 등을 활용하여 네트워크 이벤트, 악성코드 샘플 등에 대한 기본 정보, 평판 정보, 행위 등을 분석하는 업무

2 확장된 활동에 따른 방법론

예방	→	탐지	→	분석	→	대응	→	보고
정보수집				정보분석		정보공유		

위협정보 공유	• **유관기관, 전문업체에서 생산 · 배포하는 위협정보를 받거나 내부에서 생산된 위협정보를 제공하는 업무** (사이버위협정보(CTI) 공유 플랫폼 등 활용)

2 확장된 활동에 따른 방법론

기술지원	• 보안관제에 필요한 기술 및 도구를 지원하거나 정책 개발/관리 등의 업무를 수행하는 업무 • 보안관제팀에서 자체적으로 수행할 수도 있으나, 보안관제팀이 모니터링에만 집중하는 경우 모니터링 이외의 업무는 기술지원 업무로 분류

2 확장된 활동에 따른 방법론

운영	• 보안관제에 필요한 인프라 및 시스템의 상시 운영을 수행하는 업무 • 인프라 및 시스템에 대한 유지관리와 하자보수를 포함

3 보안관제 프로세스

- 보안관제를 통해 탐지된 이벤트가 오탐인 경우 관제 단계에서 자체 종결하지만, 진탐인 경우 티켓을 생성하고 이후의 프로세스 진행
  - **티켓 :** 업무의 처리에 대한 단위

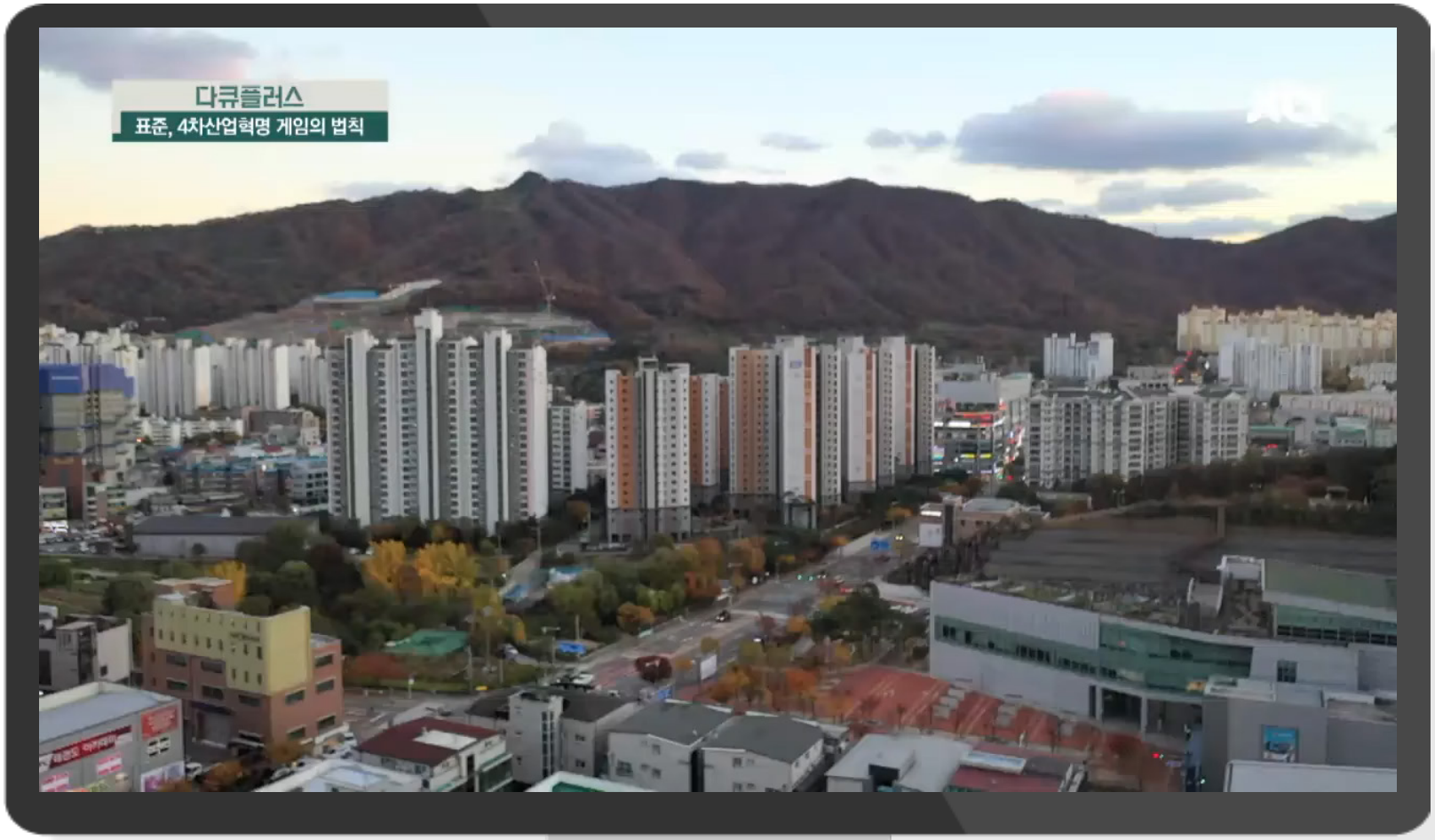
- 조사를 통해 바이러스/악성코드에 감염된 사실이 확인되는 경우, 해당 바이러스/악성코드 샘플을 채증하여 추가적인 분석을 진행
- 조사 · 분석 결과 자체적인 종결이 가능한 경우 티켓을 종결 처리
- 타 조직/기관에 의한 조사가 필요하거나 법령상 정보수사기관에 의한 수사가 필요한 경우 해당 조직/기관에 이관

IV

보안관제 관련 프레임워크

보안관제 관련 프레임워크

1 표준의 중요성



출처 다큐 플러스 - 표준, 4차 산업혁명 게임의 법칙, JTBC Entertainment(2018.11.18), https://www.youtube.com/watch?v=ZV7doXFT89o

IV 보안관제 관련 프레임워크

1 표준의 중요성

실생활 속 표준의 적용

HD TV	MPEG-2 텔레비전 방송을 위한 표준
시계	KS A ISO 80000-3 세계 표준시간
가스레인지	KS B 8115 한국산업표준
휴대폰 충전단자	IEC 62680 USB 전원연결 표준
OLED 디스플레이	KS C IEC 62341 표준
주방 싱크대 높이	SPS-KHFC 001-0438 가정용 싱크대 표준
콘센트	IEC TR 60083 220V 표준전압 표준
USB	주변장치를 연결하기 위해 사용되는 표준 연결 방식
무선 와이파이	IEEE의 802.11 무선근거리통신망 표준

출처 다큐 플러스 - 표준, 4차 산업혁명 게임의 법칙, JTBC Entertainment(2018.11.18), https://www.youtube.com/watch?v=ZV7doXFT89o

보안관제 관련 프레임워크

1 표준의 중요성

실생활 속 표준의 적용

		OLED 디스플레이	KS C IEC 62341 표준
HD TV	MPEG-2 텔레비전 방송을 위한 표준	주방 싱크대 높이	SPS-KHFC 001-0438 가정용 싱크대 표준
			준
가스레인지	한국산업표준	USB	주변장치를 연결하기 위해 사용되는 표준 연결 방식
휴대폰 충전단자	IEC 62680 USB 전원연결 표준	무선 와이파이	IEEE의 802.11 무선근거리통신망 표준

표준은 가장 기본적인 삶의 질을 보장할 수 있는 기준이자 체계로, 표준이 명확하지 않다면 이 세상은 복잡하고 혼란스럽게 될 것

출처 다큐 플러스 - 표준, 4차 산업혁명 게임의 법칙, JTBC Entertainment(2018.11.18), https://www.youtube.com/watch?v=ZV7doXFT89o

2 보안관제 업무의 표준

- **보안관제 업무가 표준화된 방식으로 수행될 수 있도록,**
  보안관제 조직과 보안관제 서비스 조직은 국제적으로 활용되는 표준 프레임워크를 토대로
  보안관제 방법론을 개발하여 활용 중
- **특히, 보안관제 전문 기업 지정 요건에 보안관제 방법론이 포함되어 있기 때문에**
  보안관제 조직과 보안관제 서비스 업체는 업무 특성을 고려 · 반영한 보안관제 방법론 확보

예 보안관제 전문기업인 이글루코퍼레이션의 경우
NIST CSF 1.1 기반의 보안관제방법론(IGMSM) 개발 · 활용

보안관제 관련 프레임워크

3 보안관제 프레임워크

보안관제 프레임워크

조직이 효과적으로 보안 위협에 대응하고 보안 관리를 수행하기 위한
지침 · 표준 · 모범 사례 · 절차들을 체계적으로 조직화한 구조

정책	절차	위험관리	모니터링	분석
사고대응 · 관리	기술 · 인프라	성과 측정	보고	

- 보안관제 프레임워크를 통해 보안 위협을 식별 · 분석 · 대응 · 복구하는 과정을 체계화 · 표준화
- 보안관제 프레임워크는 보안 위협을 효과적으로 관리 · 대응하는 포괄적인 지침과 기반 제공

3 보안관제 프레임워크

▪ 보안관제 프레임워크의 이점

① 체계적인 위험관리 접근법

② 일관된 보안 프로세스와 정책 수립

③ 신속한 사고 대응 및 복구 지원

④ 법적 요구사항 및 규제 준수

⑤ 효과적인 자원 배분

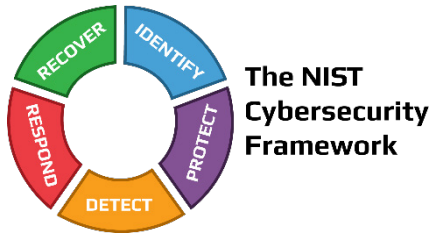
3 보안관제 프레임워크

- 주요 보안관제 프레임워크

NIST Cybersecurity Framework (CSF)

MITRE ATT&CK

MITRE D3FEND



MITRE ATT&CK™

MITRE DEFEND™

4 NIST Cybersecurity Framework (CSF)

NIST Cybersecurity Framework (CSF)

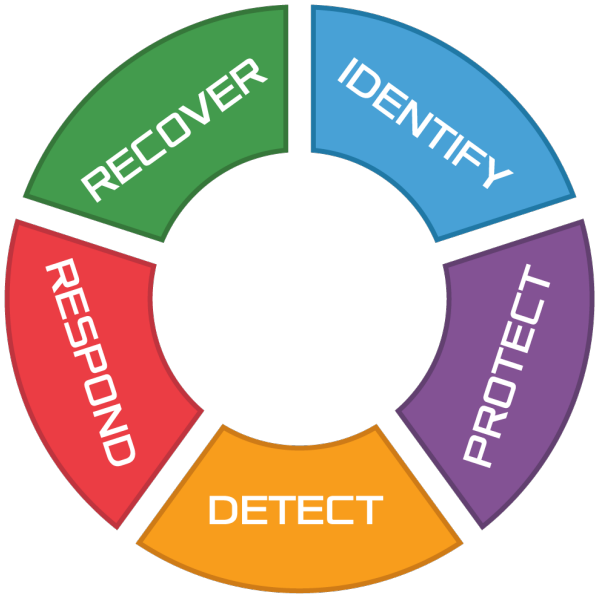
The NIST Cybersecurity Framework

미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)**에서 개발한**
사이버보안 프레임워크(Cybersecurity Framework, CSF)**는**
조직이 사이버보안 위험을 관리하는데 필요한 표준 · 지침 · 모범 사례를 제공

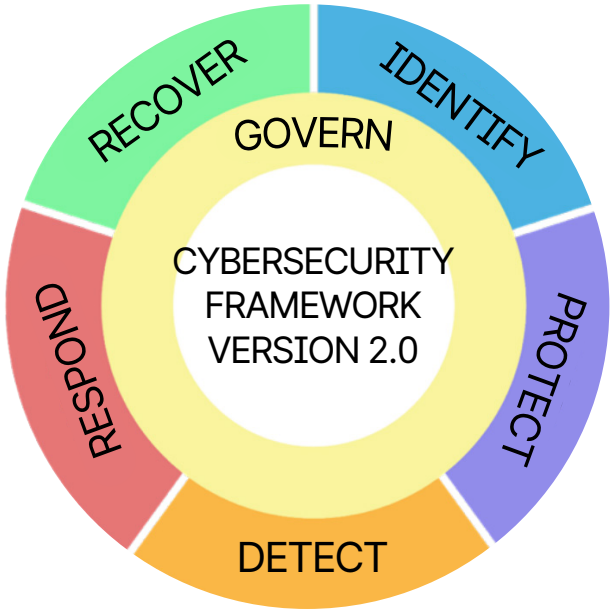
출처 Cybersecurity Framework Components, NIST, https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

4 NIST Cybersecurity Framework (CSF)

- NIST CSF는 버전 1.x 기준으로 5개의 핵심 기능으로 구성되며, 버전 2.0 기준으로는 6개의 핵심 기능으로 구성



NIST CSF 1.x



NIST CSF 2.0

출처 Cybersecurity Framework Components, NIST, https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

4 NIST Cybersecurity Framework (CSF)

- NIST CSF는 버전 1.x 기준으로 5개의 핵심 기능으로 구성되며, 버전 2.0 기준으로는 6개의 핵심 기능으로 구성

출처 Cybersecurity Framework Components, NIST, https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

4 NIST Cybersecurity Framework (CSF)

▪ NIST CSF 1.1의 기능

식별 (Identify)	보호 (Protect)	탐지 (Detect)	대응 (Respond)	복구 (Recover)
자산관리	ID관리 및 접근통제	이상징후 및 이벤트	대응계획	복구계획
업무환경	인식 및 교육	지속적 모니터링	의사소통	개선
거버넌스	데이터보안	탐지절차	분석	의사소통
위험평가	정보보호 절차		완화	
위험관리 전략	유지관리		개선	
공급망 위험관리	보호기술			

출처 Framework for Improving Critical Infrastructure Cybersecurity, NIST(2018), p. 23, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

4 NIST Cybersecurity Framework (CSF)

▪ NIST CSF 1.1의 기능

식별 (Identify)	• 시스템, 인력, 자산, 데이터 등에 대한 사이버보안 위험을 관리할 수 있도록 조직 차원의 이해 개발
보호 (Protect)	• 중요 서비스의 제공을 보장하기 위해 적절한 보호조치를 개발 · 구현
탐지 (Detect)	• 침해시도/사고의 발생을 탐지하기 위한 적절한 활동을 개발 · 구현
대응 (Respond)	• 탐지된 침해시도/사고에 대해 조치를 취하기 위한 적절한 활동을 개발 · 구현
복구 (Recover)	• 복원력을 유지하기 위한 계획을 개발 · 구현하며 침해사고로 인해 손상된 기능이나 서비스를 복구

출처 Framework for Improving Critical Infrastructure Cybersecurity, NIST(2018), p. 23, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

4 NIST Cybersecurity Framework (CSF)

▪ NIST CSF 2.0의 기능

거버넌스 (Govern)	식별 (Identify)	보호 (Protect)	탐지 (Detect)	대응 (Respond)	복구 (Recover)
조직적 맥락	자산관리	ID관리 및 접근통제	지속적 모니터링	침해관리	침해 복구계획 실행
위험관리 전략	위험평가	인식 및 교육	이상 이벤트 분석	침해분석	침해 복구 의사소통
역할과 책임	강화	데이터보안		침해대응 보고 및 의사소통	
정책		플랫폼보안		침해완화	
감시		기술 인프라 복원력			
사이버보안 공급망 위험관리					

출처 The NIST Cybersecurity Framework (CSF) 2.0, NIST(2024), p.15, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

4 NIST Cybersecurity Framework (CSF)

▪ NIST CSF 2.0의 기능

거버넌스 (Govern)	• 조직의 사이버보안 위험관리 전략 · 기대치 · 정책을 설정하여 의사소통 및 모니터링
식별 (Identify)	• 조직의 현재 사이버보안 위험을 이해
보호 (Protect)	• 조직의 사이버보안 위험을 관리하기 위한 보호조치를 사용
탐지 (Detect)	• 가능한 사이버보안 공격 및 침해시도/사고를 찾아내고 분석
대응 (Respond)	• 탐지된 사이버보안 이벤트에 대한 조치
복구 (Recover)	• 사이버보안 이벤트에 의해 영향을 받은 자산 및 운영을 복구

출처 The NIST Cybersecurity Framework (CSF) 2.0, NIST(2024), p.15, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

5 MITRE ATT&CK과 D3FEND

- MITRE Corporation은 미국 연방정부의 지원을 받으며 국가안보 관련 연구를 수행하는 비영리 연구개발 조직

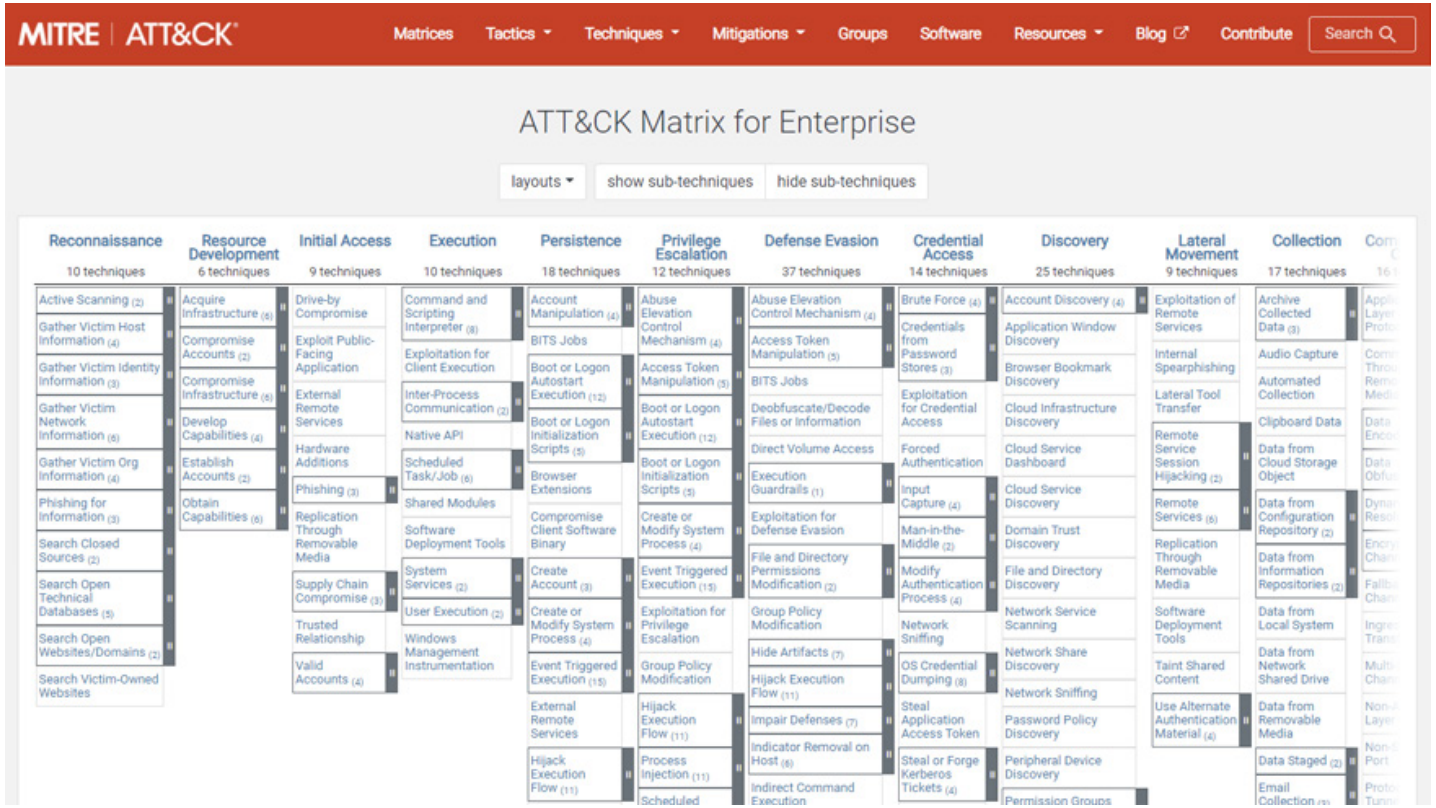
MITRE ATT&CK

- 사이버 공격자들의 공격 전술 · 기술 · 절차(TTP)를 기반으로, 공격자의 의도와 행동을 예측하는데 필요한 공격자 관점에 대한 실제적인 지식 기반을 제공하는 프레임워크
- 보안관제 조직은 MITRE ATT&CK을 활용하여 공격자 관점에서 공격자의 행동을 이해하고 이를 효과적으로 탐지 · 분석 · 대응하기 위한 전략을 개발

출처 ATT&CK Matrix for Enterprise, MITRE, https://attack.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE ATT&CK의 구성**

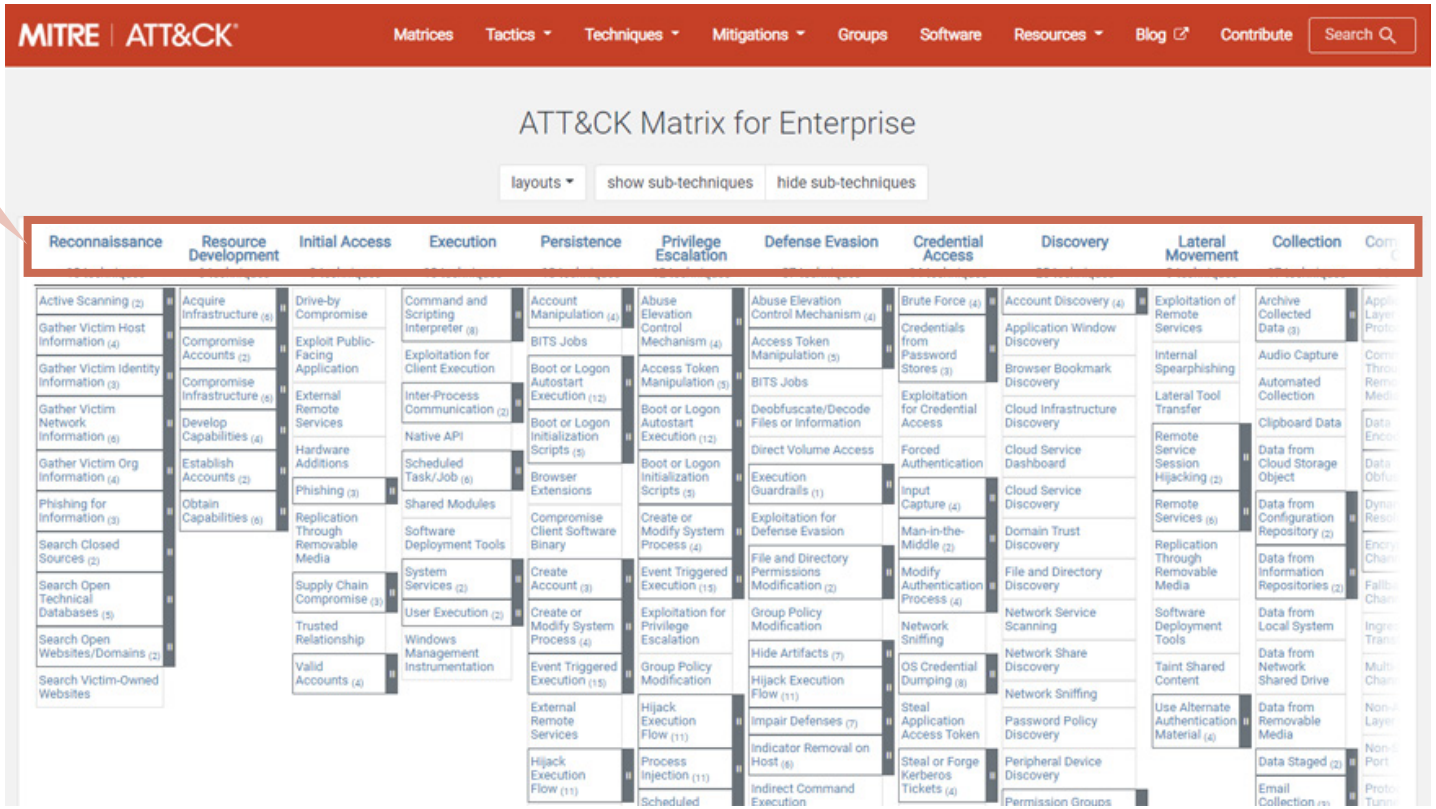


출처 ATT&CK Matrix for Enterprise, MITRE, https://attack.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE ATT&CK의 구성**

공격 전술

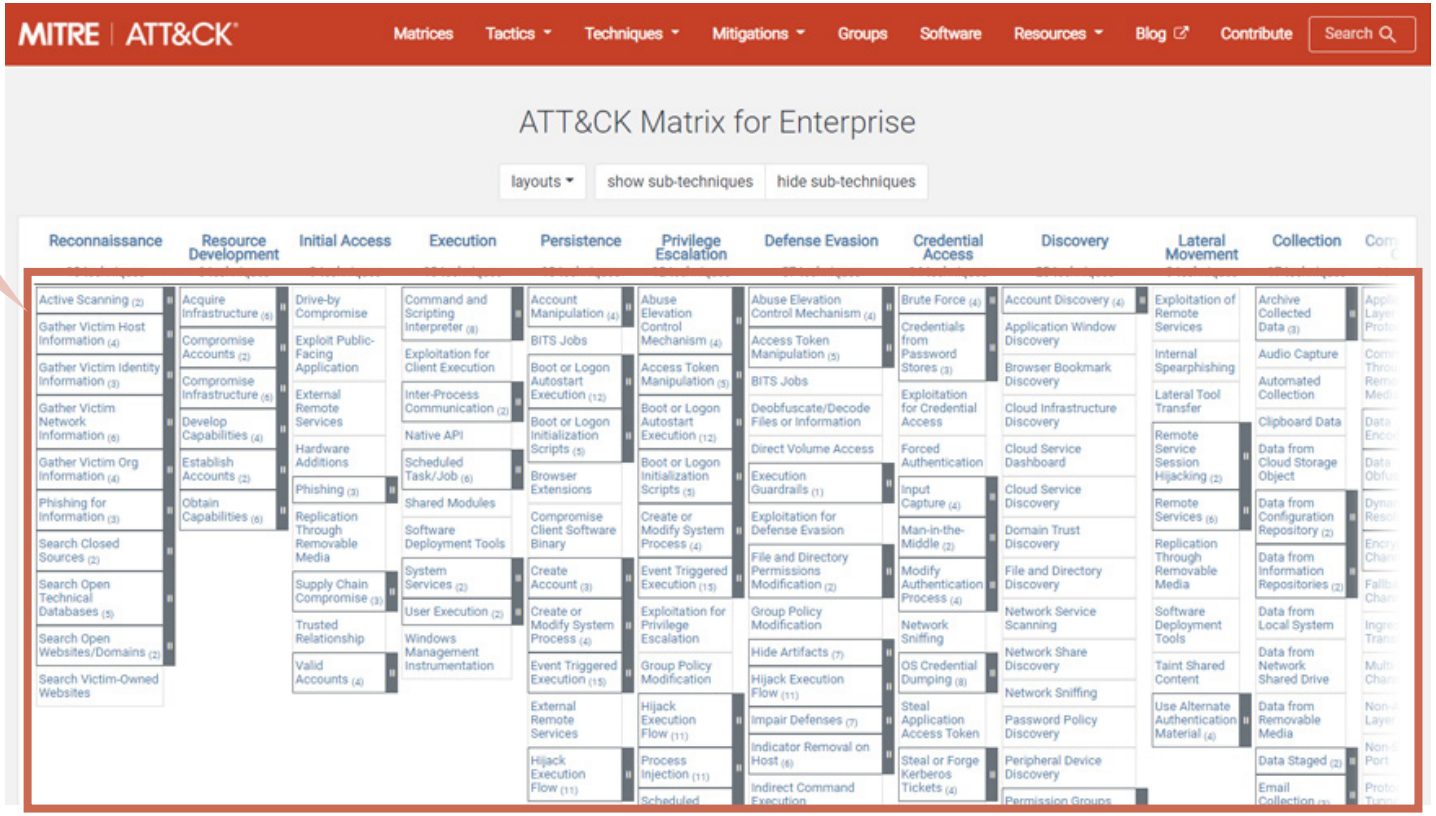


출처 ATT&CK Matrix for Enterprise, MITRE, https://attack.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE ATT&CK의 구성**

공격 기술



출처 ATT&CK Matrix for Enterprise, MITRE, https://attack.mitre.org

5 MITRE ATT&CK과 D3FEND

- MITRE Corporation은 미국 연방정부의 지원을 받으며 국가안보 관련 연구를 수행하는 비영리 연구개발 조직

MITRE D3FEND

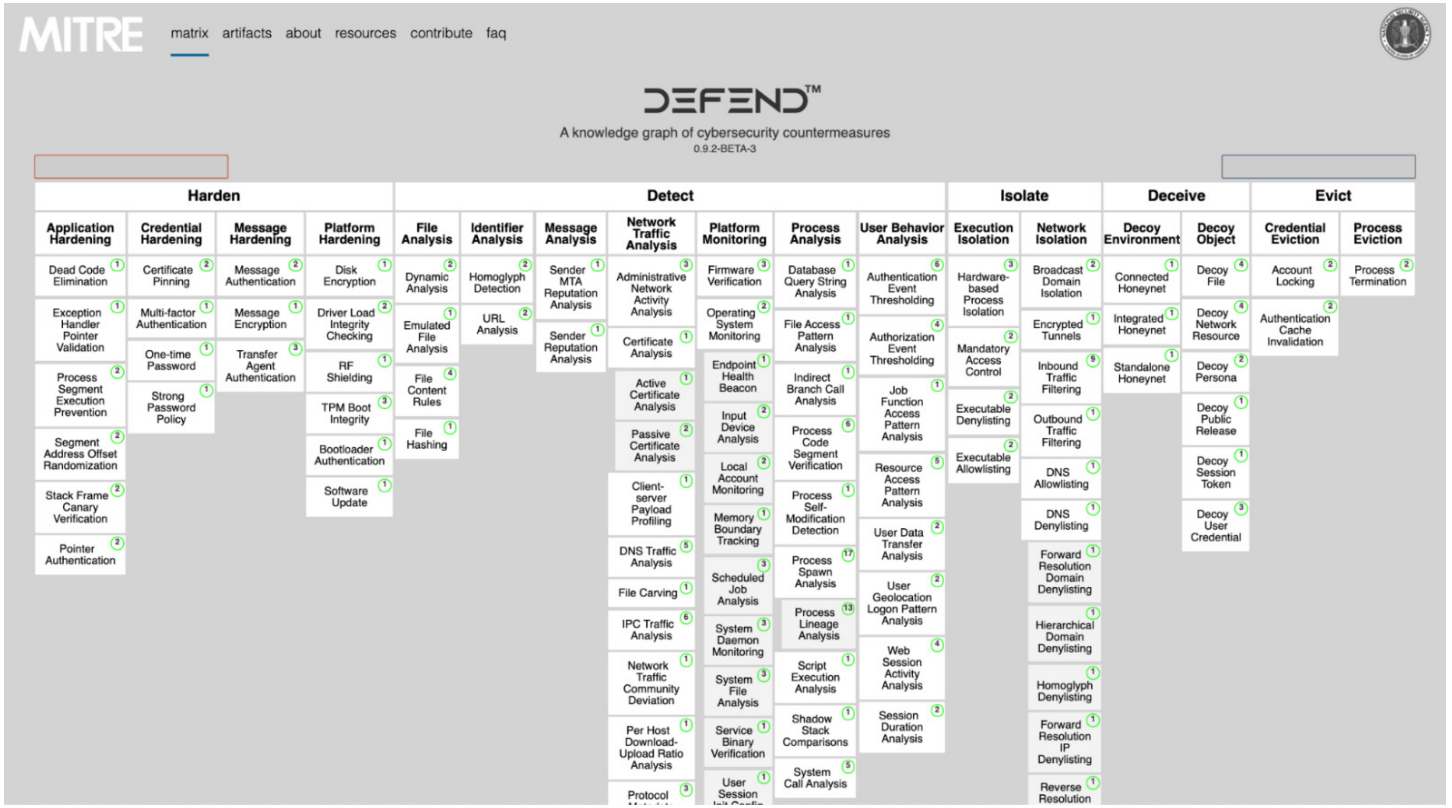
MITRE D3FEND™

- 사이버 방어 기술과 전략에 초점을 둔 프레임워크로, MITRE ATT&CK를 보완하는 방어자 관점의 프레임워크
- 사이버 방어 조치와 기술의 선택 · 구현 · 관리에 필요한 상세한 설명과 지침을 제공
- 보안관제 조직은 MITRE D3FEND를 활용하여 조직의 보안 방어 전략을 강화하고 방어 기술을 조직 내 통합

출처 D3FEND Matrix, MITRE, https://d3fend.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE D3FEND의 구성**

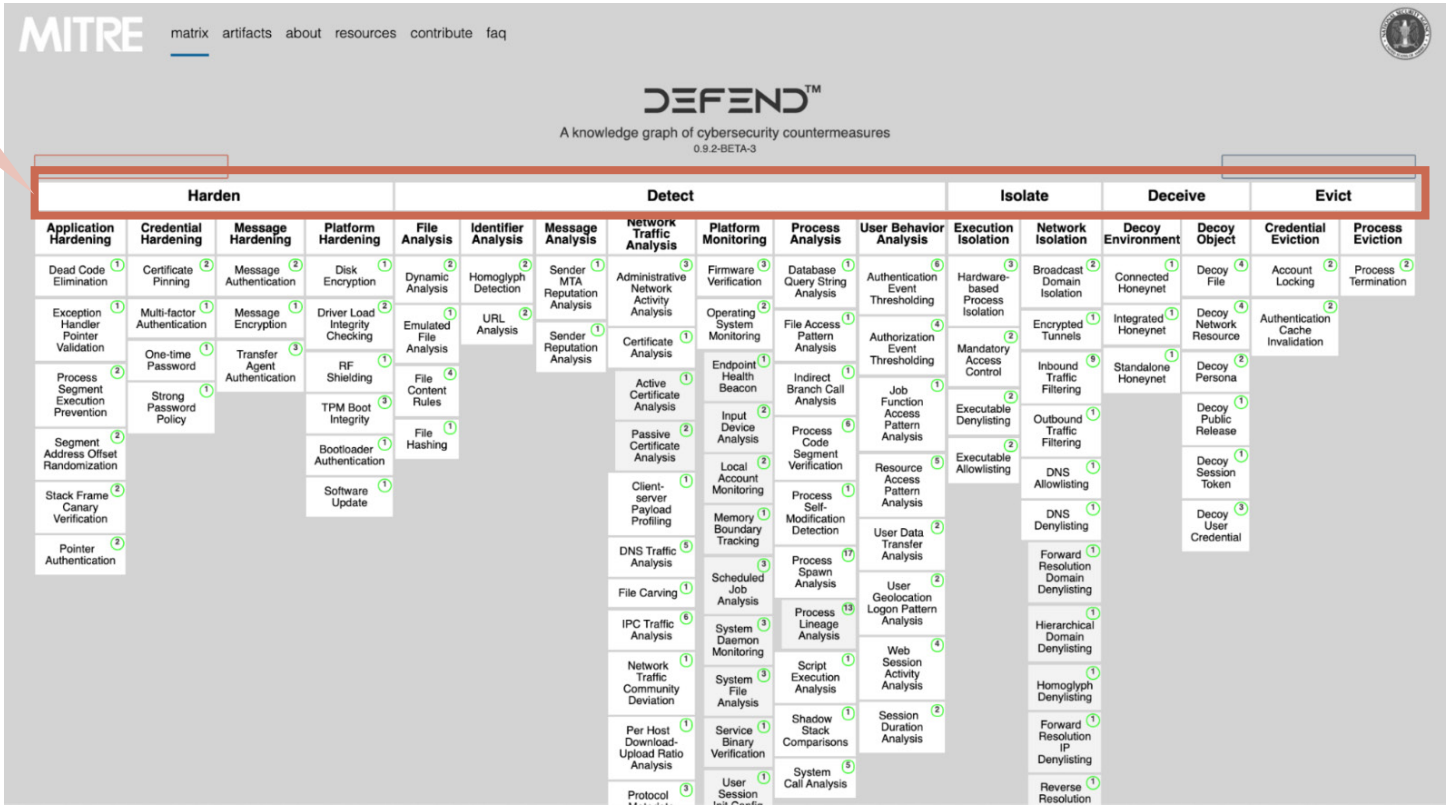


출처 D3FEND Matrix, MITRE, https://d3fend.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE D3FEND의 구성**

방어 전술

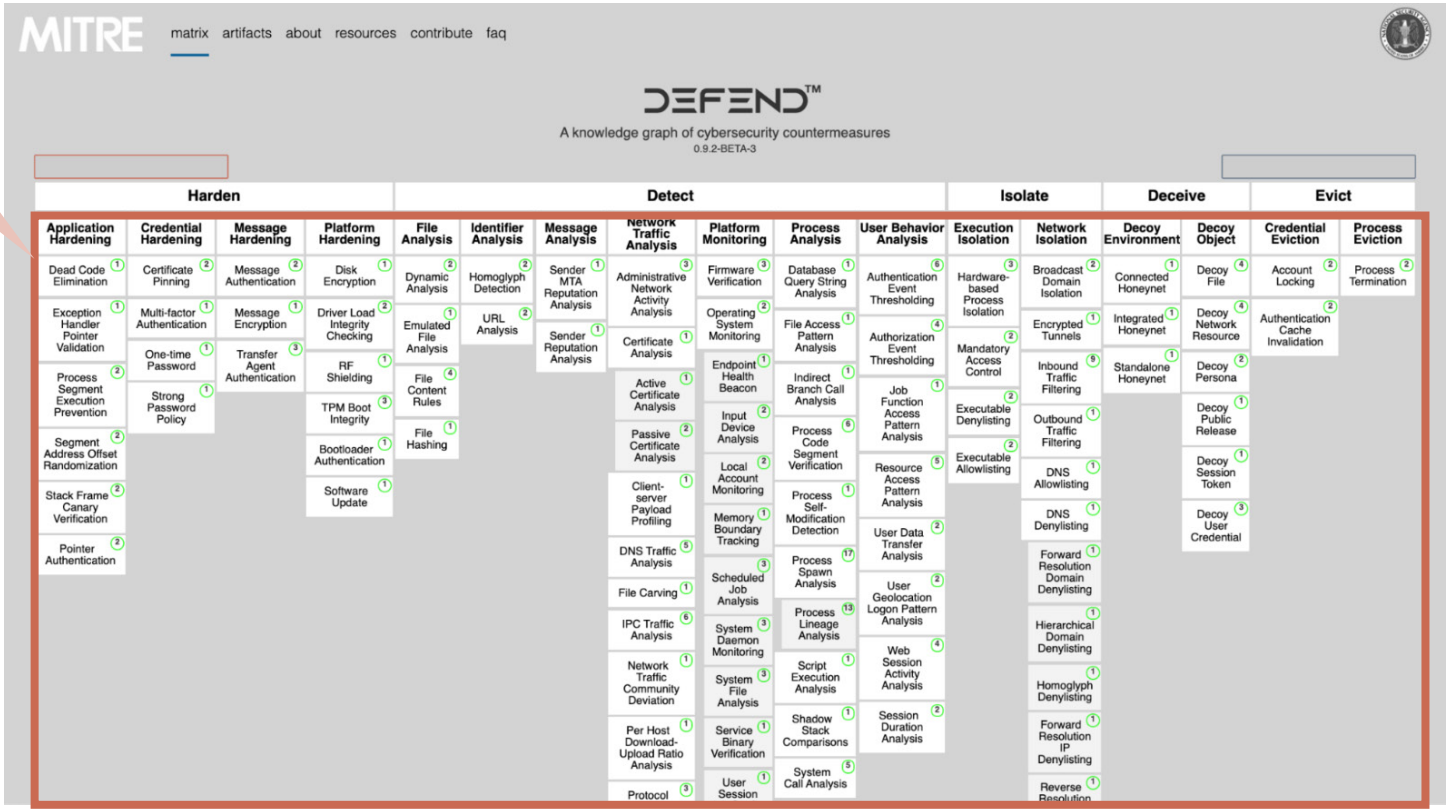


출처 D3FEND Matrix, MITRE, https://d3fend.mitre.org

5 MITRE ATT&CK과 D3FEND

- **MITRE D3FEND의 구성**

방어 기술

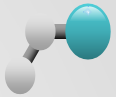


출처 D3FEND Matrix, MITRE, https://d3fend.mitre.org

요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.

요약정리



▪ 보안관제 거버넌스의 이해

• 보안관제 거버넌스

- 보안관제에 대한 의사결정 체계
- **필요성 :** 효과적인 위험 관리, 일관된 보안 프로세스와 정책, 책임 및 투명성 확보, 법적 요구사항 충족 및 규제 준수

▪ 보안관제의 유형과 보안운영 조직 구성

• 보안관제 수행 방식

- 조직의 규모 · 자원 · 특성에 따라 적절한 수행 방식을 결정하며, 수행 방식에 따라 보안관제 거버넌스에 영향
- **자체(인하우스) 보안관제 :** 직접 보안관제
- **외주(아웃소싱) 보안관제 :** 파견 보안관제, 원격 보안관제
  - * 보안관제 전문업체 지정 제도 : 보안관제 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 업체를 국가에서 지정하는 제도

요약정리

▪ 보안관제 방법론과 프로세스

• 보안관제 주요 활동

- **기본 활동**
  탐지 → 분석 → 대응
- **확장된 활동**
  예방 → 탐지 → 분석 → 대응 → 보고
  정보 수집/분석/공유
  기술지원 및 운영

• 보안운영센터의 업무 프로세스

- 보안운영센터는 보안운영센터장을 중심으로, 실시간 보안관제를 전담으로 하는 보안관제팀을 비롯하여 이외 보안운영 활동을 수행하는 팀들로 구성
  * 업무 분장 : 보안운영센터장, 보안관제팀, 조사 · 분석팀, 취약점진단/모의해킹팀, 기술지원/운영팀
- **업무 프로세스 :** 관제 → 조사 → 분석 → 이관 → 종결

요약정리

- **보안관제 관련 프레임워크**
  - **보안관제 프레임워크**
    - 보안 위협을 효과적으로 관리 · 대응할 수 있는 포괄적인 지침과 기반 제공
  - **NIST Cybersecurity Framework (CSF)**
    - 보안관제 전체 프로세스를 구조화하는데 활용
    - **1.x 기준 기능 :** 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)
    - **2.0 기준 기능 :** 1.x 기준 기능에 거버넌스(Govern) 추가
  - **MITRE ATT&CK**
    - 공격자의 행동을 이해하고 이를 탐지 · 분석 · 대응하기 위한 전략 개발 가능
  - **MITRE D3FEND**
    - 조직의 보안 방어 전략을 강화하고 방어 기술을 조직 내 통합 가능

참고문헌

- 정보통신기반보호법 (법률)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (법률)
- 사이버안보 업무규정 (대통령령)
- 국가사이버안전관리규정 (대통령훈령)
- 국가 정보보안 기본지침 (국가정보원 지침)
- 보안관제학, 2014, 안성진 등 공저, 이한미디어
- 2023 국가정보보호백서, 2023, 국가정보원 등 관계기관 합동
- 국가사이버안보센터 웹 사이트, http://www.ncsc.go.kr
- 한국인터넷진흥원 웹 사이트, http://www.kisa.or.kr
- NIST Cybersecurity Framework 2.0, https://www.nist.gov/cyberframework
- NIST Cybersecurity Framework 1.1 Archive, https://www.nist.gov/cyberframework/csf-11-archive

참고문헌

- MITRE ATT&CK 웹 사이트, http://attack.mitre.org
- MITRE D3FEND 웹 사이트, http://d3fend.mitre.org
- 사회적책임에 대한 지침(KS A ISO 26000:2010), 2021, 산업표준심의회
- 다큐 플러스 - 표준, 4차 산업혁명 게임의 법칙,
  JTBC Entertainment(2018.11.18), https://www.youtube.com/watch?v=ZV7doXFT89o

수고하셨습니다