cybereason

7000건 이상의 사고대응으로 검증한

사이버보안 필수 관리항목 11가지

사이버리즌은 수십 년간 보안 사고를 대응하면서 공격 표면을 최소화하고 탐지 • 대응 능력을 높여왔습니다. 이러한 경험을 바탕으로 사고의 영향과 손실을 줄이고, 사이버 복원력을 높이는 사이버보안 실전 가이드를 작성했습니다.
(컴플라이언스 맵핑이 포함되어 있습니다.)

왜 이 보고서가 필요할까요?

사이버 위협은 계속해서 규모와 정교함을 더해가고 있습니다. 컴플라이언스 프레임워크는 점점 더 엄격하고 복잡해지며 공급망 리스크는 상시 존재합니다. 여기에 인수합병(M&A 활동)은 새로운 보안 과제를 추가합니다. 그러나 현실은 사이버보안 예산은 늘 제한적이고, 전문가들은 과중한 업무로 번아웃에 시달리고 있습니다.

흔히 들리는 조언은 "가장 영향력이 큰 프로젝트에 집중하라"는 것이지만, 실제로 어떤 보안 통제가 가장 높은 효과를 낼까요?

많은 보안 및 리스크 리더들은 인기 있는 사이버보안 프레임워크를 답으로 제시합니다. 일부 조직은 컴플라이언스 프레임워크를 우선순위 결정의 기준으로 삼지만 기술적으로 규정을 준수하는 조직도 침해 사고를 많이 겪고 있습니다. 이 격차를 해소하기 위해 사이버리즌은 단순한 감사가 아닌 **실제 사고에서 가장 효과적인 보안 조치**를 찾고자 했습니다.

Intentional Cybersecurity와 진행한 7,000건 이상의 인시던트 조사에서 얻은 인텔리전스를 바탕으로 **실전에서 검증된 11가지 필수 사이버보안 관리항목**을 선정했습니다. 이 조치들은 피해를 최소화하고 조직이 위기 상황에서도 빠르고 효과적으로 대응 복구할 수 있도록 지원합니다.

각 조치에는 현장에서 가장 자주 발견되는 '반복되는 설정 오류와 취약점(Common Pitfalls)'이 포함되어 있으며 해당 조치가 디지털 포렌식 및 인시던트 대응(DFIR) 활동에 미치는 직접적인 영향을 명확히 보여줍니다. 또한 DFIR 관점은 기존 프레임워크에서는 볼 수 없는 실전 중심의 인사이트를 담았습니다.

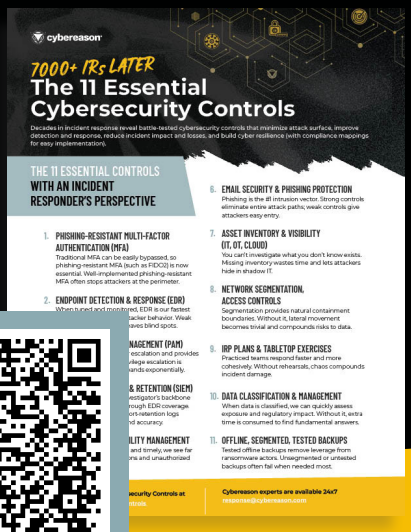
> "수천 건의 글로벌 인시던트 조사를 직접 수행하며 공격을 실제로 막는 방어책과 반복적으로 실패하는 방어책을 똑똑히 보았습니다.
>
> 이 11가지 관리항목은 그 경험을 바탕으로 조직이 실질적으로 위험을 줄일 수 있는 명확하고 우선순위화된 행동 지침을 제공합니다"

Devon Ackerman,
사이버리즌 DFIR(디지털 포렌식 및 인시던트 대응) 총괄

In partnership with INTENTIONAL CYBERSECURITY

사이버보안 필수 관리항목 11가지를 실용적으로 활용하는 방법

QR 코드를 통해 11가지 필수 사이버보안 통제를 빠르게 참조할 수 있는 데스크톱용 레퍼런스(치트시트)를 다운받을 수 있습니다.



- **리소스 우선순위화**
  실제 인시던트를 차단하는 현장 검증된 보안 조치에 투자를 집중하세요.
- **경영진 커뮤니케이션 강화**
  이 리스트를 활용해 이사회와 경영진에게 명확하게 보고하고 보안 예산을 확보하세요.
- **취약점 식별**
  현재 방어 체계를 필수 관리항목 11가지와 비교해 빠르게 약점을 찾아내세요.
- **보험 업계와 기업 내 리스크관리 기준 일치**
  보험 시장에서 인정받는 관리 대책으로 성숙도를 입증하고 위험 노출을 줄이세요.
- **인시던트 대응 준비 강화**
  테이블탑 훈련(보안 사고 시나리오 기반 모의 훈련)을 진행해 압박받는 상황에서의 복원력을 검증하세요.
- **컴플라이언스와 보안의 연결**
  효과가 높은 조치를 우선순위화하여 체크리스트를 현실적인 복원력으로 전환하세요.

#	CONTROL	CIS V8	NIST CSF	NIST 800-171
1	피싱 저항형 다중 인증 (MFA)	• 6.3 - 외부 애플리케이션 MFA 요구 • 6.5 - 관리자 접근 MFA 요구	• PR.AC-7 - 위험에 따라 인증	• 3.5.3 - 로컬 및 네트워크 접근 MFA 사용
2	엔드포인트 탐지 및 대응 (EDR)	• 10.1 - 안티멀웨어 소프트웨어 배포·유지 • 13.1 - 보안 이벤트 경보 중앙화	• DE.CM-4 - 악성코드 탐지 • RS.AN-1 - 탐지 시스템 알림 조사	• 3.14.1 - 시스템 결함 식별·보고·수정 • 3.14.5 - 정기적 시스템 스캔
3	권한 있는 액세스 관리 (PAM)	• 4.3 - 관리자 계정 접근 제어 구성 • 6.7 - Just-in-time 권한 상승 요구	• PR.AC-4 - 접근 권한 관리 • PR.AC-6 - 신원과 자격 증명 연계	• 3.1.2 - 인가된 사용자로 시스템 접근 제한 • 3.1.6 - 최소 권한 원칙 적용
4	중앙 로그 수집 및 보존 (SIEM)	• 8.2 - 감사 로그 활성화 • 8.3 - 상세 감사 로그 수집 • 8.5 - 정해진 기간 로그 보존	• DE.AE-3 - 이벤트 데이터 집계·연계 • PR.PT-1 - 감사/로그 기록 결정·문서화·구현	• 3.3.1 - 시스템 감사 로그 생성·보존 • 3.3.6 - 감사 축소·보고 생성
5	정기 패치 및 취약점 관리	• 7.3 - 공급업체 패치 적용 • 7.5 - 패치 관리 자동화	• PR.IP-12 - 취약점 관리 계획 수립·이행 • DE.CM-8 - 취약점 스캔 수행	• 3.11.2 - 취약점 스캔 • 3.14.1 - 시스템 결함 식별·보고·수정
6	이메일 보안 필터링 및 피싱 방지	• 9.1 - 피싱 차단 이메일 서버 구성 • 9.2 - DNS 필터링 서비스 사용 • 14.6 - 피싱 인지·신고 교육	• PR.AT-1 - 모든 사용자 교육 • DE.CM-7 - 무단 모바일 코드/ 이메일 첨부 모니터링 • PR.DS-2 - 전송 중 데이터 보호	• 3.1.17 - 이메일 무단 접근 보호 • 3.13.8 - 이메일 보호 메커니즘 구현 • 3.2.1 - 피싱 등 위협 인지 교육
7	자산 인벤토리 및 가시성 (IT/OT/클라우드)	• 1.1 - 상세 자산 인벤토리 구축·유지 • 1.2 - 무단 자산 처리 • 2.1 - 소프트웨어 인벤토리 구축·유지	• ID.AM-1 - 물리적 장치·시스템 인벤토리 • ID.AM-2 - 소프트웨어 플랫폼 ·애플리케이션 인벤토리 • ID.AM-4 - 외부 정보 시스템 목록화	• 3.4.1 - 기본 구성·인벤토리 구축·유지 • 3.1.1 - 인벤토리 기반 인가된 사용자 ·프로세스·디바이스 접근 제한
8	네트워크 세분화 & 접근 제어	• 3.3 - 트래픽 필터링 기반 방화벽 규칙 구성 • 14.4- 관리자·특권 접근 분할 • 12.1 - 인프라 접근 제어 중앙화	• PR.AC-5 - 네트워크 무결성 보호 • PR.PT-4 - 통신·제어 네트워크 보호	• 3.1.3 - 인가된 흐름에 따른 CUI 제어 • 3.1.20 - 외부 시스템 연결 검증·제어
9	인시던트 대응 계획(IRP) & 테이블탑 훈련	• 17.1 - 인시던트 관리 담당자 지정 • 17.2- 당국과 연락 유지 • 17.4 - 정기적 인시던트 대응 연습	• RS.RP-1 - 인시던트 발생 시 대응 계획 실행 • RS.IM-1 - 대응 전략 테스트·업데이트	• 3.6.1 - 인시던트 대응 역량 구축 • 3.6.2 - 인시던트 추적·문서화·보고 • 3.6.3 - 조직의 인시던트 대응 역량 테스트
10	데이터 분류 & 구조화된 데이터 관리	• 3.4 - 자동화 도구로 데이터 인벤토리 • 3.6 - 전송 중 민감 데이터 암호화 • 3.7 - 데이터 분류 체계 수립	• ID.RA-1 - 자산 취약점 식별·문서화 • PR.DS-1 - 정지 데이터 보호 • PR.DS-5 - 데이터 유출 방지	• 3.1.22 - 공개 시스템 내 CUI 제어 • 3.8.1 - CUI 흐름 제한에 따른 보호 • 3.8.3 - CUI 적절한 표시·라벨링
11	안전한 백업 전략: 오프라인·세그먼트 ·테스트·RTO 검증	• 11.4 - 복구 데이터 보호 • 11.5 - 정기 자동 백업 보장 • 11.6 - 주기적 복구 테스트	• PR.IP-4 - 백업 수행·보호·테스트 • PR.PT-5 - 복구 프로세스 테스트 • RC.RP-1 - 복구 계획 실행·유지	• 3.6.1 - 인시던트 대응 역량 구축 • 3.6.2 - 인시던트 추적·문서화·보고 • 3.1.1 - 백업 시스템 접근 제한

목차


1. 피싱 저항형 다중 인증 (MFA, Multi-Factor Authentication) 6


2. 엔드포인트 탐지 및 대응 (EDR, Endpoint Detection & Response) 7


3. 권한 있는 엑세스 관리 (PAM, Privileged Access Management) 8


4. 중앙 로그 수집 및 보존 (SIEM 또는 이에 준하는 솔루션) 9


5. 정기 패치 및 취약점 관리 10


6. 이메일 보안 필터링 및 피싱 방지 11


7. 자산 인벤토리 및 가시성 (IT, OT, 클라우드) 12


8. 네트워크 분할 및 접근제어 13


9. 인시던트 대응 계획(IRP, Incident Response Plans) 및 테이블탑 훈련 14


10. 데이터 분류 및 구조화된 데이터 관리 15


11. 안전한 백업 전략: 오프라인 · 세그먼트 · 테스트 · RTO 검증 16

01
피싱 저항형 다중 인증 (MFA)

다중 인증(MFA)은 사용자가 시스템이나 애플리케이션에 접근하기 전에 두 가지 이상의 인증 요소를 요구합니다. 일반적으로 비밀번호, 디바이스나 토큰, 생체 정보가 이에 해당합니다. 하지만 전통적인 MFA는 도난된 자격 증명이나 토큰 탈취 기법으로 쉽게 우회될 수 있습니다. 따라서 FIDO2와 같은 피싱 저항형 MFA를 도입하는 것이 강력히 권장됩니다. 실제 인시던트 조사에서도 공격자가 흔히 자격 증명을 탈취하거나, 피싱 키트를 이용해 손쉽게 기존 MFA 우회를 성공하고 있다는 사실이 드러났습니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ MFA가 아예 적용되지 않은 계정이 존재한다
  MFA를 적용했지만 전통적인 방식만 사용중이다
- ☐ SMS 기반 MFA만 사용한다
- ☐ VPN, RDP, 클라우드 관리자 포털 등 모든 원격 접근 경로에 MFA가 적용되지 않았다
- ☐ 임원 또는 특권 계정에 보안 예외가 허용되어 있다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

적절하게 강제된 MFA가 있으면, 공격자는 최초 침투 시도에서 벽에 부딪히게 됩니다. 이는 인시던트 대응자가 조사해야 할 계정 수를 줄이고, 침투 경로를 신속하게 격리할 수 있게 해줍니다. MFA가 약하거나 누락된 경우, 공격자의 가로 이동과 권한 상승이 쉬워지고, 침해 범위가 넓어집니다. 또한, 제대로 구현된 MFA는 위협 행위자의 활동(실패 시도, 토큰 재사용 등)을 상세하게 로깅하여, 최초 침투 지점이나 중간자 공격을 더 빠르고 정확하게 추적할 수 있습니다.

프레임워크	컴플라이언스 맵핑
CIS v8	6.3 – 외부 애플리케이션 MFA 요구 6.5 – 관리자 접근 MFA 요구
NIST CSF	PR.AC – 7 – 위험에 따라 인증
NIST 800-171	3.5.3 – 로컬 및 네트워크 접근 MFA 사용

02
엔드포인트 탐지 및 대응 (EDR)

EDR(Endpoint Detection & Response) 솔루션은 워크스테이션, 서버, 때로는 클라우드 워크로드 등 엔드포인트의 활동을 지속적으로 모니터링하여, 프로세스 인젝션, 가로 이동, 자격 증명 탈취 등 의심스러운 행위와 이상 징후를 탐지 · 조사 · 대응합니다. EDR은 방어자에게 공격자의 행동을 실시간 및 과거 이력까지 투명하게 보여주며, 전통적인 백신이나 경계 기반 방어를 우회하는 최신 공격에도 신속하게 대응할 수 있는 핵심 도구입니다. 실제 인시던트 대응 현장에서는 EDR이 조기에 침입을 탐지하고, 신속하게 격리 · 차단하는 데 결정적인 역할을 합니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ EDR이 설치되어 있지만 경보 피로(alert fatigue), 튜닝 부족, 약한 트리아지로 탐지 실패가 발생한다
- ☐ EDR이 모든 엔드포인트에 일관되게 배포되지 않아 레거시 시스템 · 클라우드 · 테스트/개발 네트워크 · 미관리 디바이스 등에서 가시성에 빈틈이 있다
- ☐ 경보 규칙이 제대로 조정되지 않아 중요한 이벤트가 누락되거나 과도한 경보로 인해 대응이 지연된다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

EDR은 네트워크 환경 전반에서 공격자의 행동을 가장 빠르게 파악할 수 있는 수단입니다. 초기 침입부터 횡적 이동, 권한 상승 시도까지 모든 과정을 추적할 수 있으며 올바르게 배포 · 모니터링된 EDR은 격리까지의 시간을 획기적으로 단축시킵니다. 반면 EDR 커버리지가 불완전하거나 경보가 무시되면 조사 속도가 느려지고 보안 사각지대가 생겨 공격자가 더 깊숙이 침투할 수 있습니다.

프레임워크	컴플라이언스 맵핑
CIS v8	10.1 – 안티멀웨어 소프트웨어 배포 · 유지 13.1 – 보안 이벤트 경보 중앙화
NIST CSF	DE.CM–4 – 악성코드 탐지 RS.AN–1 – 탐지 시스템 알림 조사
NIST 800-171	3.14.1 – 시스템 결함 식별 · 보고 · 수정 3.14.5 – 정기적 시스템 스캔

03
권한 있는 액세스 관리 (PAM)

PAM(Privileged Access Management)은 고가치 시스템, 계정, 데이터에 대한 접근을 엄격하게 통제하는 보안 전략입니다. Just-in-time 권한 부여, 자격 증명 금고화, 세션 모니터링, 접근 승인 등 다양한 기능을 통해 관리 또는 민감 기능에 대한 접근을 제한합니다. 공격자는 횡적 이동, 방어 무력화, 민감 데이터 접근을 시도할 때 특정 권한이 있는 계정을 가장 먼저 노립니다. 효과적인 PAM은 침해 발생 시 피해 범위를 최소화하고, 공격자가 도메인 전체를 장악하는 것을 차단할 수 있습니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 네트워크 전반에 과도하게 많은 관리자 권한 계정이 존재한다
- ☐ 로컬 관리자 계정을 여러 명이 공유하거나, 약한 비밀번호 또는 MFA 미적용 상태로 운영한다
- ☐ 자격 증명 회전(주기적 변경), 특권 세션 로깅, 누가 언제 무엇에 접근했는지에 대한 감사를 수행하지 않는다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

PAM이 제대로 적용된 환경에서는 특정 권한이 있는 계정의 활동에 대한 명확한 감사 추적이 가능해 신속한 격리와 공격자 확산 억제가 가능합니다. 이는 인시던트 대응팀이 공격자의 권한 상승과 가로 이동을 늦추고, 탐지 및 대응 시간을 확보하는 데 큰 도움이 됩니다.

반대로 PAM이 미흡하면, 공격자는 손쉽게 권한을 상승시키고 네트워크 내 여러 시스템으로 빠르게 확산할 수 있으며, 조사 과정도 훨씬 복잡해집니다.

프레임워크	컴플라이언스 맵핑
CIS v8	4.3 – 관리자 계정 접근 제어 구성 6.7 – Just-in-time 권한 상승 요구
NIST CSF	PR.AC-4 – 접근 권한 관리 PR.AC-6 – 신원과 자격 증명 연계
NIST 800-171	3.1.2 – 인가된 사용자로 시스템 접근 제한 3.1.6 – 최소 권한 원칙 적용

04
중앙 로그 수집 및 보존 (SIEM 또는 이에 준하는 솔루션)

운영체제, 핵심 애플리케이션, 네트워크 및 엣지 장비(방화벽, VPN 등)에서 발생하는 로그를 SIEM이나 데이터 레이크 플랫폼에 중앙화하여 수집 · 보존하는 것은 인시던트 대응, 규제 준수, 전사적 사이버 복원력 확보에 필수적입니다. SIEM 기반 플랫폼은 심층 분석을 통해 더 빠른 탐지와 포렌식 조사를 가능하게 하며, 중앙 로그가 없으면 의미 있는 패턴을 놓치게 되어 대응팀이 추가 로그 소스를 찾아야 하므로 분석 범위와 정확도가 떨어집니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ PowerShell, 인증 이벤트, 클라우드 관리자 활동 등 핵심 로그가 누락되어 있다
- ☐ 로그는 수집하지만 보존 기간이 너무 짧다
- ☐ 경보 규칙이 제대로 튜닝되지 않아 경보 피로(alert fatigue) 또는 보안 사각지대가 발생한다
- ☐ 로그 수집 · 보존 비용 부담으로 데이터 볼륨 관리에 어려움이 있다
- ☐ 로그 정책 수립 및 운영에 전문가의 가이드가 부족하다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

중앙 로그는 인시던트 조사의 근간입니다. 로그를 통해 타임라인을 재구성하고, 최초 감염 지점(Patient Zero)을 식별하며, 공격자의 행위를 시스템 전반에 걸쳐 상관 분석할 수 있습니다.

로그가 누락되거나 사일로화되어 있으면, 조사 속도가 느려지고 정확도가 떨어집니다. 적절한 로그 보존과 가시성은 대응 속도와 심층 분석의 수준을 결정짓는 핵심 요소입니다.

프레임워크	컴플라이언스 맵핑
CIS v8	8.2 – 감사 로그 활성화 8.3 – 상세 감사 로그 수집 8.5 – 정해진 기간 로그 보존
NIST CSF	DE.AE – 3 – 이벤트 데이터 집계 · 연계 PR.PT – 1 – 감사/로그 기록 결정 · 문서화 · 구현
NIST 800-171	3.3.1 – 시스템 감사 로그 생성 · 보존 3.3.6 –감사 축소 · 보고 생성

05
정기 패치 및 취약점 관리

정기 패치 및 취약점 관리는 시스템, 서버, 네트워크 장비, 애플리케이션 전반에 걸쳐 취약점을 식별하고, 우선순위를 정해 신속하게 보완하는 프로세스입니다.패치가 적용되지 않은 취약점은 공격자에게 가장 신뢰할 수 있는 침투 경로를 제공합니다. 실제 인시던트 조사에서도 취약점 악용은 항상 상위 3대 침입 원인에 포함됩니다. 적시에 패치를 적용하면 공격 표면을 줄이고, 기회주의적 침입 시도를 사전에 차단할 수 있습니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 최신 자산 인벤토리가 없어 보안 사각지대가 존재한다
- ☐ 패치 주기가 느리거나 위험도가 높은 자산이 패치 대상에서 누락된 적이 있다
- ☐ 취약점 스캔만하고 신속한 보완 조치가 이루어지지 않는다
- ☐ 하이브리드 환경(온프레미스/클라우드 등)에서 패치 상태를 일관되게 추적하지 못한다
- ☐ 위험 기반 우선순위 적용이 미흡해 영향도가 큰 취약점(CVE)이 다른 이슈에 묻혀 방치된다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

패치 및 취약점 관리가 성숙한 조직에서는 예방 가능한 인시던트가 현저히 줄어듭니다. 조사 과정에서도 이미 알려진 취약점(CVE) 악용 사례를 쫓느라 시간을 낭비하지 않아 대응 속도가 빨라집니다.

반대로, 패치 관리가 미흡하면 공격자는 오래된 취약점을 이용해 빠르게 침투하고, 네트워크 내에서 신속하게 확산할 수 있습니다.

프레임워크	컴플라이언스 맵핑
CIS v8	7.3 – 공급업체 패치 적용 7.5 – 패치 관리 자동화
NIST CSF	PR.IP–12 – 취약점 관리 계획 수립 · 이행 DE.CM–8 – 취약점 스캔 수행
NIST 800-171	3.11.2 – 취약점 스캔 3.14.1 – 시스템 결함 식별 · 보고 · 수정

06
이메일 보안 필터링 및 피싱 방지

이메일 보안 필터링 및 피싱 방지 조치는 피싱, 악성코드, 도메인 스푸핑 등 악의적인 이메일을 탐지하고 차단하는 기술과 프로세스를 포함합니다. 일반적으로 보안 이메일 게이트웨이, DNS 필터링, DMARC 정책 적용, 사용자 신고 메커니즘 등이 결합되어 운영됩니다. 피싱과 소셜 엔지니어링은 공격자들이 선호하는 대표적인 공격 방식이며 2025년 상반기 Cybereason IR 사례 중 46%를 차지했습니다. 효과적인 이메일 보안은 위협을 사용자에게 도달하기 전에 차단하여 자격 증명 탈취, 악성코드 유포, 비즈니스 이메일 침해(BEC) 등 다양한 공격을 사전에 방지합니다.

*DMARC(Domain-based Message Authentication, Reporting and Conformance): 이메일 스푸핑과 같은 사기 메일을 막기 위한 이메일 인증 프로토콜

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 이메일 정책이 느슨해져 고도화된 피싱 메일에 취약하다
- ☐ 도메인에 DMARC가 정책 수준으로 적용되지 않았거나 SPF · DKIM이 누락 또는 From 주소와 불일치한다
- ☐ 사용자 신고 프로세스가 제대로 작동하지 않는다
- ☐ 피싱 모의훈련이 일관성 없이 시행되거나 아예 없다
- ☐ 이메일 보안 시스템이 인시던트 탐지 체계와 연동되지 않는다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

강력한 이메일 보안 조치는 공격 경로 전체를 차단할 수 있습니다. 이메일 보안이 제대로 적용된 환경에서는 피싱 기반 침해가 현저히 줄어들고, 초기 침입 및 가로 이동이 제한됩니다.
반대로, 이메일 보안이 미흡하면 공격자는 자격 증명 탈취, 악성코드 전달, 지속적 침투 등 다양한 방식으로 조직을 위협할 수 있습니다.
또한, 이메일 보안 솔루션은 관련 로그를 생성하여, 공격 대상과 위험 데이터 식별 등 인시던트 조사에 중요한 단서를 제공합니다.

*SPF(Sender Policy Framework): 이메일 발신자 도메인의 위변조를 막는 이메일 인증 기술
*DKMI(DomainKeys Identified Mail): 발신 메일의 진위 여부와 무결성을 확인하는 이메일 인증방법

프레임워크	컴플라이언스 맵핑
CIS v8	9.1 – 피싱 차단 이메일 서버 구성 9.2 – DNS 필터링 서비스 사용 14.6 – 피싱 인지 · 신고 교육
NIST CSF	PR.AT-1 – 모든 사용자 교육 DE.CM-7 – 무단 모바일 코드/이메일 첨부 모니터링 PR.DS-2 – 전송 중 데이터 보호
NIST 800-171	3.1.17 – 이메일 무단 접근 보호 3.13.8 – 이메일 보호 메커니즘 구현 3.2.1 – 피싱 등 위협 인지 교육

07
자산 인벤토리 및 가시성 (IT, OT, 클라우드)

조직 전반의 하드웨어, 소프트웨어, 가상 머신, 클라우드 서비스, OT/IoT 자산을 최신 · 정확하게 파악하고, 속성 · 상태 · 소유 · 보안 상태까지 관리하는 것은 사이버보안의 기본입니다. 보이지 않으면 보호할 수 없습니다. 공격자는 관리되지 않거나 미확인 · 미감시 시스템을 노려 침투하며, 특히 하이브리드 IT/OT와 클라우드 중심 환경에서 그 위험이 커집니다. 견고한 자산 가시성은 패치, 접근 제어, 탐지, 인시던트 대응의 기초 체력을 형성합니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 자산 인벤토리가 불완전하거나 수작업으로 유지되어 정확성이 떨어진다
- ☐ 네트워크 엔지니어링 · IT · 정보보안 · 개발/운영 등 부서별로 인벤토리가 사일로로 분리되어 있다
- ☐ 섀도우 IT로 인한 보안 사각지대가 있다
- ☐ 자산에 중요도, 포함 데이터, 의존성, 소유자 태그가 없어 대응 우선순위와 위험 자산 파악이 어렵다
- ☐ 자산 탐지 도구가 서로 연동되지 않거나 핵심 인프라 밖의 영역을 충분히 스캔하지 못한다

*섀도우 IT(Shadow IT): 조직의 공식 IT 부서의 승인, 지식, 또는 통제 없이 직원들이 개별적으로 사용하는 소프트웨어, 하드웨어, 애플리케이션, 시스템

DFIR(디지털 포렌식 & 인시던트 대응) 관점

조사 시 무엇이 어디에 존재하는지를 정확히 아는 것은 범위 확정과 격리 속도를 획기적으로 높입니다. 인벤토리가 불완전하면 대응팀은 알려지지 않은 엔드포인트나 고객조차 인지하지 못한 클라우드 리소스를 찾느라 소중한 시간을 소모하게 됩니다.

반대로 우수한 자산 가시성은 경보 · 로그 상관분석의 정확도를 높여, 탐지 · 대응 의사결정을 빠르고 정밀하게 만들어 줍니다.

프레임워크	컴플라이언스 맵핑
CIS v8	1.1 – 상세 자산 인벤토리 구축 · 유지 1.2 – 무단 자산 처리 2.1 – 소프트웨어 인벤토리 구축 · 유지
NIST CSF	ID.AM-1 – 물리적 장치 · 시스템 인벤토리 ID.AM-2 – 소프트웨어 플랫폼 · 애플리케이션 인벤토리 ID.AM-4 – 외부 정보 시스템 목록화
NIST 800-171	3.4.1 – 기본 구성 · 인벤토리 구축 · 유지 3.1.1 – 인벤토리 기반 인가된 사용자 · 프로세스 · 디바이스 접근 제한

08
네트워크 세분화 & 접근 제어

네트워크를 민감도, 비즈니스 기능, 신뢰 수준에 따라 분리하고 각 영역 간 접근을 엄격하게 통제하는 것은 공격자의 내부 확산을 효과적으로 차단하는 실질적 방어 전략입니다. 이러한 세분화는 방화벽, 접근 제어 목록(ACL), 가상 네트워크(VLAN), 클라우드 네이티브 세분화 등 다양한 방식으로 구현할 수 있습니다. 네트워크 세분화와 접근제어는 침해 발생 시 피해 범위를 최소화하고 기업의 핵심 자산을 안전하게 보호하며 공격의 확산 속도를 효과적으로 늦춥니다. 특히, 특정 시스템 · 서비스 · 계정만이 민감 영역에 접근할 수 있도록 엄격히 제한하는 접근제어는 아이덴티티 기반 보안과 권한 있는 액세스 관리(PAM)의 강력한 보안 체계의 토대가 됩니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 네트워크가 과도하게 개방적이며 중요 시스템과 일반 사용자 네트워크 간 분할이 부족하다
- ☐ 방화벽 규칙이 오래되어 있거나 기본값이 '모두 허용'으로 설정되어 있다
- ☐ 클라우드 환경에서 IAM(Identity & Access Management) 역할이나 보안 그룹 설정이 과도하게 넓다
- ☐ 분할이 외부 경계에만 집중되어 있고 내부 이동 경로에 대한 통제가 부족하다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

네트워크 세분화가 잘된 환경에서는 자연스러운 격리 경계가 형성되어 공격자가 일반 사용자 PC를 침해하더라도 재무, 인사, IT 관리, 백업 등 특정 업무 영역으로의 확산이 어렵습니다.

반대로 세분화가 미흡하면 공격자는 네트워크 내에서 빠르고 광범위하게 이동할 수 있어 인시던트 대응팀이 전체 환경을 격리해야 하는 상황까지 발생할 수 있습니다.

프레임워크	컴플라이언스 맵핑
CIS v8	3.3 – 트래픽 필터링 기반 방화벽 규칙 구성 14.4 – 관리자 · 특권 접근 분할 12.1 – 인프라 접근 제어 중앙화
NIST CSF	PR.AC – 5 – 네트워크 무결성 보호 PR.PT – 4 – 통신 · 제어 네트워크 보호
NIST 800-171	3.1.3 – 인가된 흐름에 따른 CUI 제어 3.1.20 – 외부 시스템 연결 검증 · 제어

09
인시던트 대응 계획(IRP) & 테이블탑 훈련

인시던트 대응 계획(IRP, Incident Response Plans)은 사이버 사고 발생 시 역할, 책임, 커뮤니케이션 프로토콜, 기술적 대응 절차를 명확히 정의하는 공식 문서입니다. 테이블탑 훈련은 실제 공격 시나리오를 가정해 IRP를 테스트하고 프로세스의 허점과 가정의 타당성을 검증하며 법무 · IT · 홍보 · 경영진 등 주요 이해관계자 간 협업을 강화하는 훈련입니다. 위기 상황에서 대응이 분산되면 시간과 비용이 증가하고, 혼란이 피해를 증폭시킵니다. 잘 준비된 IRP와 반복적인 테이블탑 훈련은 조직의 대응 속도와 일관성을 높이고 비즈니스 영향 최소화에 결정적인 역할을 합니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 대응 계획이 오래되었거나 테스트되지 않았거나, 단순히 컴플라이언스 체크박스용으로 작성되어 있다.
- ☐ 계획이 지나치게 기술적이거나, 반대로 너무 모호해 실제 의사결정(규제기관 통보, 시스템 차단 등)에 대한 명확한 책임자가 없다
- ☐ 테이블탑 연습이 과도하게 각본화되어 있거나, 법무 · 홍보 · 경영진 등 핵심 이해관계자가 참여하지 않는다
- ☐ 연습 후 교훈이 제대로 기록 · 반영되지 않는다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

인시던트 대응을 한 번이라도 실전처럼 연습한 조직은 실제 사고 발생 시 훨씬 빠르고 일관되게 대응합니다. 접근 권한이나 승인 대기 시간에 소모되는 시간이 줄어들고, 침입 확산을 신속하게 차단할 수 있습니다.

반대로 대응 계획이 없거나, 팀이 리허설을 해본 적이 없다면, 대응 과정이 혼란스러워지고 그 혼란이 피해를 더욱 키우게 됩니다.

프레임워크	컴플라이언스 맵핑
CIS v8	17.1 – 인시던트 관리 담당자 지정 17.2 – 당국과 연락 유지 17.4 – 정기적 인시던트 대응 연습
NIST CSF	RS.RP–1 – 인시던트 발생 시 대응 계획 실행 RS.IM–1 – 대응 전략 테스트 · 업데이트
NIST 800-171	3.6.1 – 인시던트 대응 역량 구축 3.6.2 – 인시던트 추적 · 문서화 · 보고 3.6.3 – 조직의 인시던트 대응 역량 테스트

10
데이터 분류 & 구조화된 데이터 관리

데이터의 민감도, 가치, 규제 요건에 따라 식별 · 분류하고 라이프사이클 전반에 걸쳐 관리 · 보호 · 거버넌스를 적용하는 것은 보안의 핵심입니다. 이러한 데이터 분류와 관리는 접근제어(8. 네트워크 및 권한 관리)를 강화하고 인시던트 대응과 규제 준수를 지원하는 핵심 요소입니다. 공격자는 파일 서버, 데이터베이스, SharePoint 폴더 등에서 지적재산, 재무정보, 개인정보 등 핵심 데이터를 빠르게 찾아내기에 데이터가 어디에 있고, 어떻게 보호되고 있는지 명확히 파악하는 것은 위험을 줄이는 첫걸음입니다.

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 조직이 민감 데이터의 위치를 명확히 파악하지 못한다
- ☐ 데이터 분류 작업이 수동, 정적, 또는 실제 보안 통제와 연계되지 않는다
- ☐ 구조화된 데이터(예: 데이터베이스)는 관리하지만, 비구조화 데이터(파일 공유, 클라우드 스토리지)는 관리하지 않는다
- ☐ 태깅, 암호화, 보존 정책이 누락되거나 일관성 없이 적용된다

DFIR(디지털 포렌식 & 인시던트 대응) 관점

데이터가 잘 분류되어 있으면 인시던트 발생 시 위험 범위를 빠르게 파악하고, 규제 통보 및 법적 노출 여부를 신속히 판단할 수 있습니다. 반대로 데이터 분류가 미흡하면 대응팀은 공격자가 규제 대상 데이터를 접근했는지 확인하기 위해 많은 시간을 소요하게 됩니다.

예를 들어 공격자가 마케팅 자료 서버만 암호화했다는 사실을 안다면 과연 몸값을 지불할 필요가 있을까요?

프레임워크	컴플라이언스 맵핑
CIS v8	3.4 – 자동화 도구로 데이터 인벤토리 3.6 – 전송 중 민감 데이터 암호화 3.7 – 데이터 분류 체계 수립
NIST CSF	ID.RA–1 – 자산 취약점 식별 · 문서화 PR.DS–1 – 정지 데이터 보호 PR.DS–5 – 데이터 유출 방지
NIST 800-171	3.1.22 – 공개 시스템 내 CUI 제어 3.8.1 – CUI 흐름 제한에 따른 보호 3.8.3 – CUI 적절한 표시 · 라벨링

11
안전한 백업 전략:
오프라인 · 세그먼트 · 테스트 · RTO 검증

이상적인 백업은 일정 기간 동안 관리자나 침해된 시스템조차도 수정 · 삭제 · 암호화할 수 없는 불변(immutable) 데이터 복사본을 보유하는 것입니다. 오프라인 · 세그먼트 백업은 랜섬웨어 시나리오에서 최후의 방어선으로 매우 중요하지만 유일한 보안 전략이 되어서는 안 됩니다. 백업은 인시던트 이후 복구를 지원하는 조치이며 나머지 10가지 관리항목이 공격 예방과 피해 최소화에 더 직접적인 효과를 발휘합니다.

*RTO(Recovery Time Objective): 사이버 공격으로 시스템이 중단된 후 정상 서비스로 복구하는 데 걸리는 최대 허용 시간

보안 담당자를 위한 체크리스트: 반복되는 설정 오류 & 취약점

- ☐ 백업이 온라인 상태로 운영되어 동일 네트워크로 연결된 시스템과 함께 위협에 노출된다.
- ☐ 백업이 RTO를 충족하지 못하거나 테스트가 부족하다.
- ☐ 백업 빈도만 관리하고 실제 복구 가능성은 점검하지 않는다.
- ☐ 랜섬웨어 암호화, 데이터 유출 등 비상 상황을 가정한 복구 절차 훈련을 거의 하지 않는다.

DFIR 관점

실제로 백업이 암호화되거나 삭제되어 복구가 지연되거나 불가능해지는 사례가 자주 발생합니다. 오프라인 · 세그먼트 · 테스트된 백업은 랜섬웨어 공격자의 협상력을 크게 약화시키며 경영진에게 더 많은 해결방안 선택지를 제공합니다. 복구 시간과 효과는 이러한 환경에서 현저히 개선됩니다.

프레임워크	컴플라이언스 맵핑
CIS v8	11.4 – 복구 데이터 보호 11.5 –정기 자동 백업 보장 11.6 – 주기적 복구 테스트
NIST CSF	PR.IP–4 – 백업 수행 · 보호 · 테스트 PR.PT–5 – 복구 프로세스 테스트 RC.RP–1 – 복구 계획 실행 · 유지
NIST 800-171	3.6.1 –인시던트 대응 역량 구축 3.6.2 – 인시던트 추적·문서화·보고 3.1.1 – 백업 시스템 접근 제한

cybereason DOOSAN

사이버 복원력의 다음 단계로 나아가세요

Cybereason 전문가들은 수천 건의 인시던트에 대응한 경험을 바탕으로 귀사의 보안 프로그램이 필수 관리 항목 11가지를 벤치마킹할 수 있도록 지원합니다.

오늘 바로 Cybereason 전문가와 1:1 세션을 예약하세요:
response@cybereason.com.

[솔루션 문의]
(주)두산 디지털이노베이션BU
ddi.marketing@doosan.com

THE IR TEAM

7,000+
인시던트 조사

300+
엘리트 전문가

500+
테이블탑 연습

100+
자격증(예: CREST, SANS, OSCP 등) 보유